

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX, INC.

Petitioner,

v.

LAURI VALJAKKA

Patent Owner

IPR2023-00423

U.S. Patent No. 10,726,102

**DECLARATION OF PAUL D. MARTIN IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW OF U.S. PATENT NO. 10,726,102**

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	Introduction	1
II.	Qualifications and Expertise	3
III.	Understanding of Relevant Legal Principles	11
IV.	Background	14
A.	Technical Background.....	14
1.	Cryptography	14
2.	Digital Rights Management	17
B.	The '102 Patent	21
C.	Prosecution History	28
D.	Level of Ordinary Skill in the Art.....	30
E.	Claim Construction	31
1.	<i>“Fingerprint”</i>	32
2.	Order of Steps	33
V.	GROUND 1: Claim 10 is Obvious Over Downs.	36
A.	Overview of Downs.....	36
1.	Downs’ System	37
2.	Overview of Distribution Flow	41
B.	Independent Claim 10	45
1.	Preamble [10P].....	46
2.	<i>“Obtaining an access restricted content”</i> [10A].	47
3.	<i>“Fingerprint”</i> Limitations	49

4.	<i>“Access[ing] Restricted Content”</i>	55
VI.	GROUND 2: Claims 10-11 Are Obvious Over DeMello, Schwartz, and Walmsley.....	61
A.	Overview of the Combination	61
1.	DeMello	61
2.	Schwartz.....	75
3.	Walmsley	80
4.	Motivation to Combine	81
B.	Independent Claim 10	85
1.	Preamble [10P].....	86
2.	<i>“Obtaining an access restricted content”</i> [10A].	87
3.	<i>“Fingerprint”</i> Limitations	91
4.	<i>“Access[ing] Restricted Content”</i>	95
C.	Dependent Claim 11	101
VII.	Conclusion.....	103

I. Introduction

1. I have been retained by Perkins Coie LLP on behalf of Netflix (“Netflix” or “Petitioner”), to provide this Declaration concerning technical subject matter relevant to the petition for *Inter Partes* Review (“Petition”) of U.S. Patent 10,726,102 to Valjakka, et al (“the ’102 patent”).

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have reviewed and am familiar with the specification and the claims of the ’102 patent. In general, I will cite to the specification of a United States patent using the following formats: (Patent No., Col:Line Number(s)) or (Patent No., Paragraph Number(s)). For example, the citation (’102 patent, 1:1-10) points to the ’102 patent specification at column 1, lines 1-10. Also, for convenience, I use italics to denote limitations from the challenged claims.

4. All of the opinions contained in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming the opinions expressed in this Declaration, I reviewed the documents listed below.

- U.S. Patent 10,726,102 to Valjakka (“the ’102 patent”; NF-1001)
- File History of the ’102 patent (NF-1002)
- U.S. Patent 6,226,618 to Downs, et al (“Downs”; NF-1005)
- U.S. Patent 6,891,953 to DeMello, et al (“DeMello”; NF-1006)

- U.S. Patent 8,112,444 to Schwartz, et al (“Schwartz”; NF-1007)
- U.S. Patent 7,685,424 to Walmsley, et al (“Walmsley”; NF-1008)
- Schneier, “Applied Cryptography” (1996) (“Schneier”; NF-1009)
- S.R. Subramanya and Byung K. Yi, “Digital Rights Management,” IEEE Potentials, March/April 2006 (“Subramanya”; NF-1010)
- Rosenblatt, et al, “Digital Rights Management: Business and Technology”, M&T Books, 2002 (“Rosenblatt”; NF-1011)
- Excerpt from Webster’s Encyclopedic Unabridged Dictionary of the English Language (2001) (Definition of “Fingerprint”) (NF-1012)
- Claim Construction Order in Valjakka v. Netflix, Inc., 22-cv-01490 (December 13, 2022) (NF-1013)
- Krawczyk, et al, RFC2014, “HMAC: Keyed-Hashing for Message Authentication”, IETF, Network Working Group, February 1997 (NF-1014)

I have also reviewed and am familiar with the other materials referred to in this Declaration. To the best of my knowledge, the documents listed above are true and accurate copies of what they purport to be and are the kinds of materials that an individual with expertise in this field at the relevant time period would reasonably rely on in formulating opinions, such as those set forth in this declaration

5. I have been asked to provide my technical opinions regarding how a person of ordinary skill in the art (“POSITA”) would have understood the claims of the ’102 patent at the time of the alleged invention. For purposes of whether the teachings of the prior art render the claims of the ’102 patent obvious, I have been asked to assume the date of January 8, 2014—the filing date of the listed Foreign

Priority Application, FI20145013. I have also been asked to provide my technical opinions on how concepts in the '102 patent specification relate to claim limitations of the '102 patent. In reaching the opinions provided herein, I have considered the '102 patent, its prosecution history, and the references cited above and have drawn as appropriate on my own education, training, research, knowledge, and personal and professional experience.

II. Qualifications and Expertise

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, education, experience, and publications is set forth in my curriculum vitae ("CV"), which is provided as NF-1004.

7. I have personal knowledge of the facts and opinions set forth in this declaration and believe them to be true. If called upon to do so, I would testify competently thereto. I have been warned that willful false statements and the like are punishable by fine or imprisonment, or both.

8. I am being compensated for my time in connection with this *inter partes* review proceeding at my standard consulting rate. I am also being reimbursed for expenses that I incur during the course of this work. My compensation is not contingent upon the results of my study and analysis, the substance of my opinions, or the outcome of any proceeding involving the challenged claims. I have no

financial interest in the outcome of this matter of in any litigation involving the '102 patent.

9. I am a Senior Research Scientist and the Director of Firmware Security at Harbor Labs, a provider of software and hardware expertise and services. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science.

10. I began working in the software industry in 2008, when I obtained my first independent consulting client—Brandeis University. I created a program for their computer repair shop's ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets in order to easily identify customers' devices.

11. Shortly after finishing my engagement with Brandeis University, I began working for the Johns Hopkins University Digital Research and Curation Center as a student programmer. There, I created a batch importer for a digital archiving system called DSpace in order to enable hundreds of digitally archived works per week to automatically be added to the repository. I next ported a web interface for statistics tracking and visualization to the same digital archiving system in order to allow library staff to more easily visualize and understand data about how the digital archiving system was being used through a common web-based interface.

12. In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for IOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. I worked for ISE as an intern throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

13. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, and I began researching computer security and privacy systems in order to both design novel technologies for securing computing systems

and to also bridge the interface gap between users and their technology. As such, my research focused not only on developing technical solutions to novel security and privacy systems but to also presenting these solutions in a way that non-technical users could understand.

14. During my tenure as a Ph.D. student at Johns Hopkins, I was fully funded as a research assistant and/or teaching assistant throughout all of my semesters. I was a member of the Upsilon Pi Epsilon computer science honor society. I was also a member of the Johns Hopkins chapter of the Association for Computing Machinery. I earned an award for outstanding teaching assistant in the Computer Science department for the year 2014-2015. I co-instructed a short course called, “Introduction to Hardware Hacking,” with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification, network traffic analysis; and web-based vulnerability assessment and exploitation

15. I represented Johns Hopkins University as a student speaker at numerous open houses and admitted student days to help introduce prospective students to the computer science department. I was selected to speak to the external advisory board for the computer science department to provide insight into the student

experience in the department. I served the department as the faculty liaison czar for several semesters, in which I attended and documented faculty meetings, which I then summarized for the students in the department. I also mentored and supervised a high school student on a year-long student project in software design and I supervised a variety of undergraduate research assistants on some of my research projects.

16. I finished my Ph.D. by successfully defending my dissertation, entitled "Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare," on February 12, 2016. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation and error-proofing of security controls.

17. During my doctorate and afterwards, I have produced, peer reviewed, and published research in areas such as fingerprinting, anomaly detection, multifactor authentication and embedded systems security. In many of these cases, I focused not only on designing novel security systems but also on designing usable web-based security systems for controlling them and understanding their data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which

was funded in part by Accenture Labs, I developed a Hadoop-based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed web application to automatically produce human-readable reports and graphs for use in consulting. Accenture subsequently patented this technology.

18. Similarly, in my work at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a SmartGrid network as well as to detect unexpected anomalies in the network. Applied Communication Sciences subsequently patented this work and continued to build on the project. To my knowledge, they actually sold and/or still sell this product as part of their SecureSmart Managed Security Service product offering.

19. I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies, especially in healthcare settings. In one project, I and my co-authors designed an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of in order to be used as a secondary authentication mechanism for accessing patient medical

records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical records of nearby patients. In another project, I and my co-authors designed an authentication bracelet that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. Upon use of other terminals throughout the hospital, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal in order to allow the user to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user.

20. My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection and automated security enforcement. In one case, I designed a security system that can be soldered directly to the CPU of embedded devices in order to perform control-flow integrity for purposes of profile building and enforcement. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices in order to build a software profile of the platform configuration of the device which can then be cross-referenced with a vulnerability database. I have also written a patent on this specific technique.

21. In February 2016, I joined Harbor Labs full-time as a research scientist. In January 2019, I was promoted to senior research scientist. At Harbor Labs, I manage client engagements and lead teams in the areas of security analysis and source code analysis.

22. A substantial portion of my role at Harbor Labs is in supervising source code review teams as part of legal consulting engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling in the millions or billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms and countless other products.

23. I am also the technical and development lead for a firmware security analysis engine for a product that we are developing called Firmware IQ. Firmware IQ is designed to analyze the firmware of embedded devices for security vulnerabilities in an automated fashion. In one configuration of the product, a developer uploads a firmware image to a web-based portal which uses a broker to forward the firmware to an engine for analysis. The engine unpacks the firmware, breaks it into its constituent components, and then performs more than a hundred automated security checks in order to find vulnerabilities in the firmware image.

The results are then reported through JSON to a web-based presentation system which displays them in an interactive fashion.

24. A more detailed list of my engagements at Harbor Labs can be found on my attached CV.

III. Understanding of Relevant Legal Principles

25. I am not a lawyer and will not provide any legal opinions. Although I am not a lawyer, I have been advised that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

26. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

27. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called “secondary

considerations” of non-obviousness if they are present. Such secondary considerations include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; and the patentee proceeded contrary to the accepted wisdom of the prior art. I am not aware of any evidence of secondary considerations of non-obviousness relevant to the '696 patent. I reserve the right to supplement this Declaration if Patent Owner introduces evidence of secondary considerations of non-obviousness.

28. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

- (1) identify the particular references that, singly or in combination, make the patent obvious;
- (2) specifically identify which elements of the patent claim appear in each of the asserted references; and
- (3) explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the

inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:

- combining prior art elements according to known methods to yield predictable results;
- simple substitution of one known element for another to obtain predictable results;
- use of known technique(s) to improve similar devices (methods or products) in the same way;
- applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
- “obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
- known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predictable to a person of ordinary skill in the art; and
- some teaching, suggestion, or motivating in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

29. I have been informed that, in considering obviousness, hindsight reasoning derived from the patent-at issue may not be used.

IV. Background

30. The '102 patent “relates generally to a method of using digital rights management keys to provide access to access restricted content.” (NF-1001, '102 patent, 1:8-10.) The '102 patent therefore combines well-known concepts in cryptography with well-known concepts in digital rights management.

A. Technical Background

1. Cryptography

31. The art and science of keeping messages secure is referred to as cryptography. (NF-1009, Schneier, 1.) A message is referred to as plaintext. (*Id.*) The process of disguising the message to hide its substance is known as encryption and the encrypted message is commonly referred to as ciphertext. (*Id.*) The process of turning ciphertext back into plaintext is known as decryption. (*Id.*)

32. Cryptography can provide confidentiality, authentication, and integrity for a message. (NF-1009, Schneier, 2.) Disguising a message through encryption can provide confidentiality to the message so that non-authorized parties (parties without a key that can decrypt the encrypted content) cannot view, access, or use the content. Cryptography can provide authentication allowing the receiver of a message to ascertain its origin to prevent an intruder from masquerading as the message originator. (*Id.*) Cryptography can also provide integrity permitting the receiver of a message to verify that the message and/or portions of the message's

contents have not been modified in transit or a false message substituted for the legitimate message. (*Id.*)

33. An encryption algorithm, also referred to as a cipher, is a mathematical function used for encryption and decryption. (NF-1009, Schneier, 2.) There are two general types of key-based algorithms: symmetric algorithms and public-key algorithms. (NF-1009, Schneier, 4.)

34. **Symmetric Algorithms:** Symmetric algorithms use the same key to encrypt and decrypt data. (*See* NF-1005, Downs, 12:46-48; *see also*, NF-1009, Schneier, 4.) In these algorithms, the “data sender and the message recipient must share the key.” (NF-1005, Downs, 12:48-49.) The shared key is referred to as a symmetric key. (NF-1005, Downs, 12:49-50.) Available symmetric algorithms available before January 2014 include DES, RC2 and RC4. (NF-1005, Downs, 12:54.) Another well-known algorithm prior to January 2014 was AES.

35. **Asymmetric (Public Key) Algorithms:** Asymmetric (Public) key algorithms use two keys that “are mathematically related so that data encrypted with one key can only be decrypted with the other key.” (NF-1005, Downs, 13:22-25; *see also*, NF-1009, Schneier, 4.) One key is kept private (private key) and the other key is distributed publicly (public key). (*See* NF-1005, Downs, 13:25-26.) For secure message transmission, the sender uses the recipient’s public key to encrypt the message. (*See* NF-1005, Downs, 13:27-28.) Only the recipient with the

associated private key can decrypt the message (NF-1005, Downs, 13:29-30.)

Asymmetric (Public) key algorithms are also used to generate digital signatures using the private key. (*See* NF-1005, Downs, 13:31-32.) Prior to 2014, RSA was a commonly used public-key algorithm (NF-1005, Downs, 13:34-35) and remains so today.

36. Digital Signature: Digital signatures are generally used to protect the integrity of a message or data within a message. One way to create a digital signature is for a message originator to compute the message digest and encrypt the message digest using the originator's private key. (*See* NF-1005, Downs, 13:51-54.) For example, a "one-way hash algorithm is used to calculate a message digest." (NF-1005, Downs, 14:6-7.) "A hash algorithm takes a variable-length-input message and converts it into a fixed length string, the message digest." (NF-1005, Downs, 14:7-9.) Common one-way hash functions include SHA256. The computed message digest is then encrypted using the private key of the originator. (NF-1005, Downs, 13:52-54.) The message is distributed with its signature. (NF-1005, Downs, 13:54-55.) The recipient verifies the digital signature first by decrypting the signature using the public key of the message originator to recover the message digest. (NF-1005, Downs, 13:55-58.) The recipient then computes the digest of the received message and compares it to the decrypted version. (NF-1005, Downs, 13:58-60.) If the message has not been altered (i.e., the message integrity

is confirmed), the calculated digest and recovered digest will be the same. (NF-1005, Downs, 13:60-62.)

37. **Certificate:** A certificate is a digital document issued by certification authority that binds a public key to a person or entity. (NF-1005, Downs, 14:21-23.) The certificate includes the public key, the name of the person or entity, an expiration date, the name of the certification authority, and other information. (NF-1005, Downs, 14:23-25.) The certificate also includes the digital signature of the certification authority. (NF-1005, Downs, 14:25-27.)

2. Digital Rights Management

38. Digital rights management (DRM) “broadly refers to a set of policies, techniques and tools that guide the proper use of digital content.” (NF-1010, Subramanya, 31.) Figure 1 from Subramanya, reproduced below, illustrates a high-level view of the components and flow of content in a DRM system. The DRM content creator “is mainly concerned with the core data/information that goes into the content.” (*Id.*) The creator passes the raw content to a producer which processes the content and generates packaged content, including adding metadata associated with the content. (*Id.*) The consumer “is the ultimate user of the content.” (*Id.*)

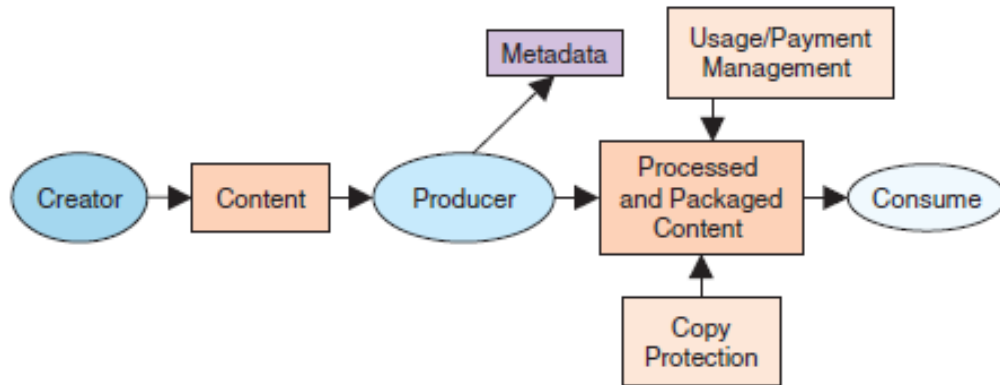


Fig. 1 Broad overview of flow of content from creator to consumer

39. One primary design philosophy of a DRM system “is the separation of content from the rights.” (NF-1010, Subramanya, 32.) Employing this technique in a DRM system “allows the content to be distributed or downloaded freely.” (*Id.*) In DRM systems, content “cannot be consumed without a valid license.” (*Id.*) As shown in Figure 3 of Subramanya, the license “contains the rights object” and “the key required to unlock the content in case it is protected.” (NF-1010, Subramanya, 33.)

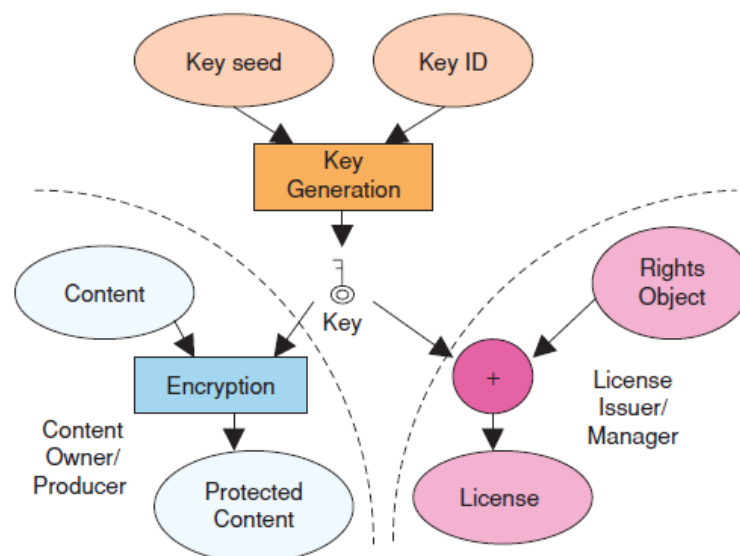
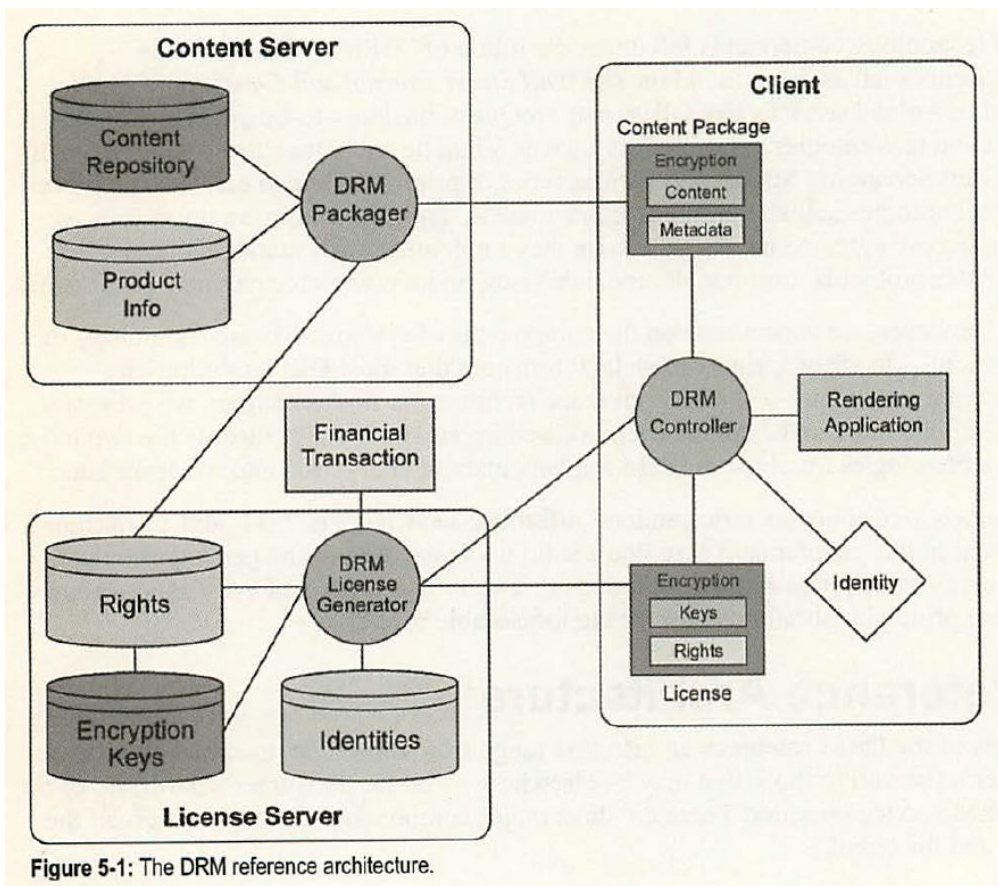


Fig. 3 Key generation and use of key in content protection and license generation

40. The basic components of a DRM system were known for over a decade prior to the '102 patent. The three major components of a DRM system are the content server, the license server, and the client, illustrated in Figure 5-1 from Rosenblatt (reproduced below). The content repository at the content server “is a collection of content that’s either in suitable format for distribution through the DRM system or (as depicted in Figure 5-1) can be put into the correct format on demand.” (NF-1011, Rosenblatt, 80.) The content repository (e.g., a file server or database server) “contains content as well as *metadata*, or information about the content.” (*Id.* (emphasis in original).)



41. A typical sequence of events inherent in DRM is illustrated in Rosenblatt, Figure 5-2 below. First, a user obtains content and makes a request to exercise rights on the content (e.g., the right to play the content on the user's device). (NF-1011, Rosenblatt, 83.) The DRM controller on the user device "gathers information necessary for generating a license." (*Id.*) The DRM controller "sends the identity and content information in a request to the license server." (NF-1011, Rosenblatt, 84) The license generator authenticates the client's identity and "uses the content identifier to look up rights information about the content." (*Id.*) The license generator "pulls together rights information, client identity information, and encryption keys (7), and creates a license-which is itself encrypted or at least tamperproofed." (*Id.*) The license is then returned to the client which uses the license to decrypt content and release it to the user's application. (*Id.*)

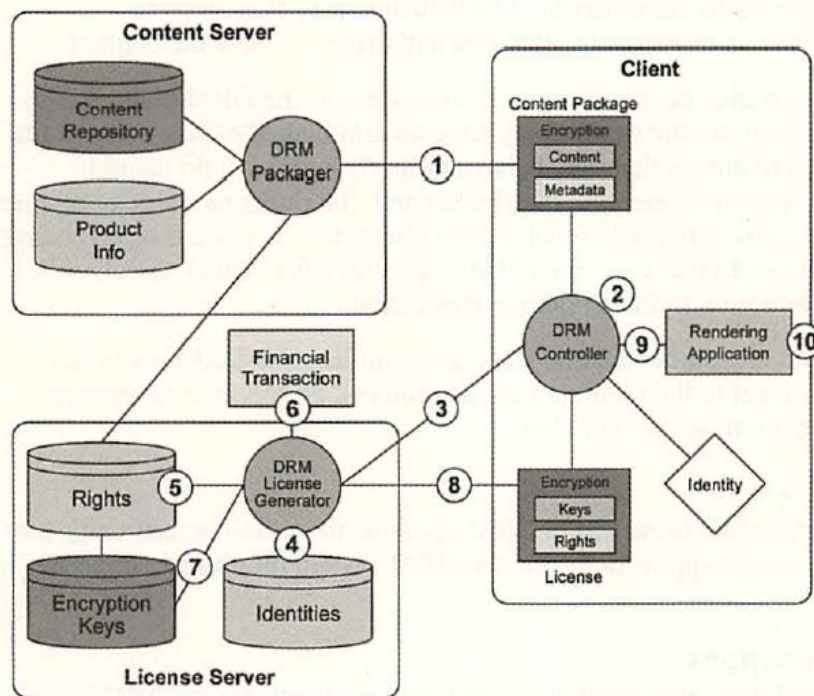


Figure 5-2: Sequence of events in exercising rights to content.

B. The '102 Patent

42. The system of the '102 patent, illustrated in Figure 1 below, illustrates the network topology for providing access to access restricted content to a user. (NF-1001, 4:43-45.) The network includes a “communication device 12 belonging to or used by a user (not shown) who intends to obtain access to access restricted content.” (NF-1001, 5:19-21.) The access restricted content “may be stored in a database” labeled 14. (NF-1001, 5:33-35.) The network further includes a content access authorization server 22. (NF-1001, 5:64-65.) The authorization server 22 includes an interrogation module 26, validation module 28, calculation module 30 and decryption module 32. (NF-1001, 6:1-3.)

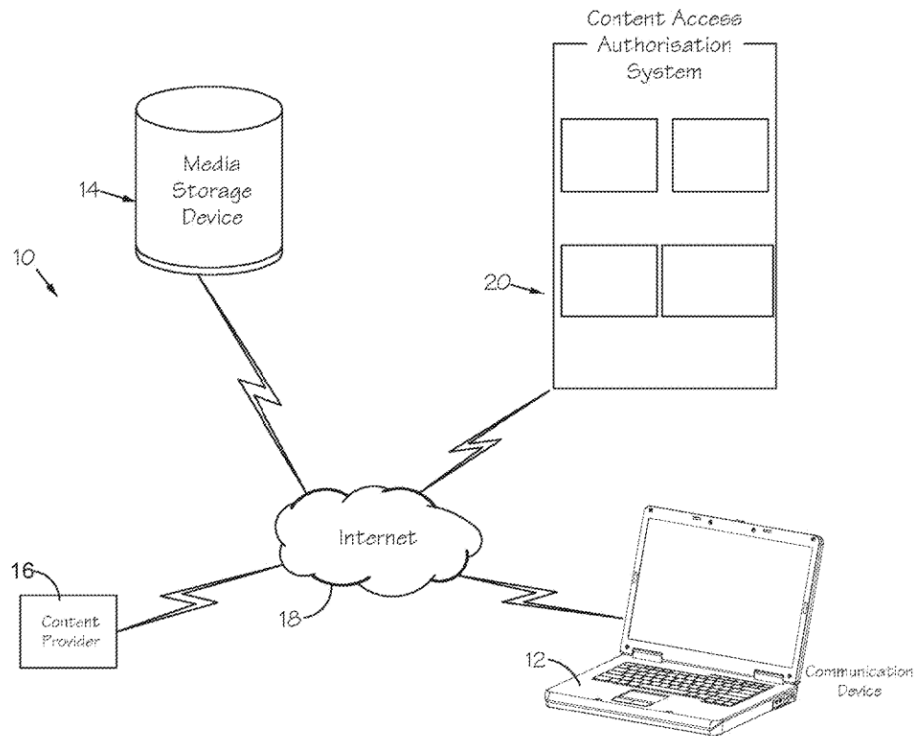
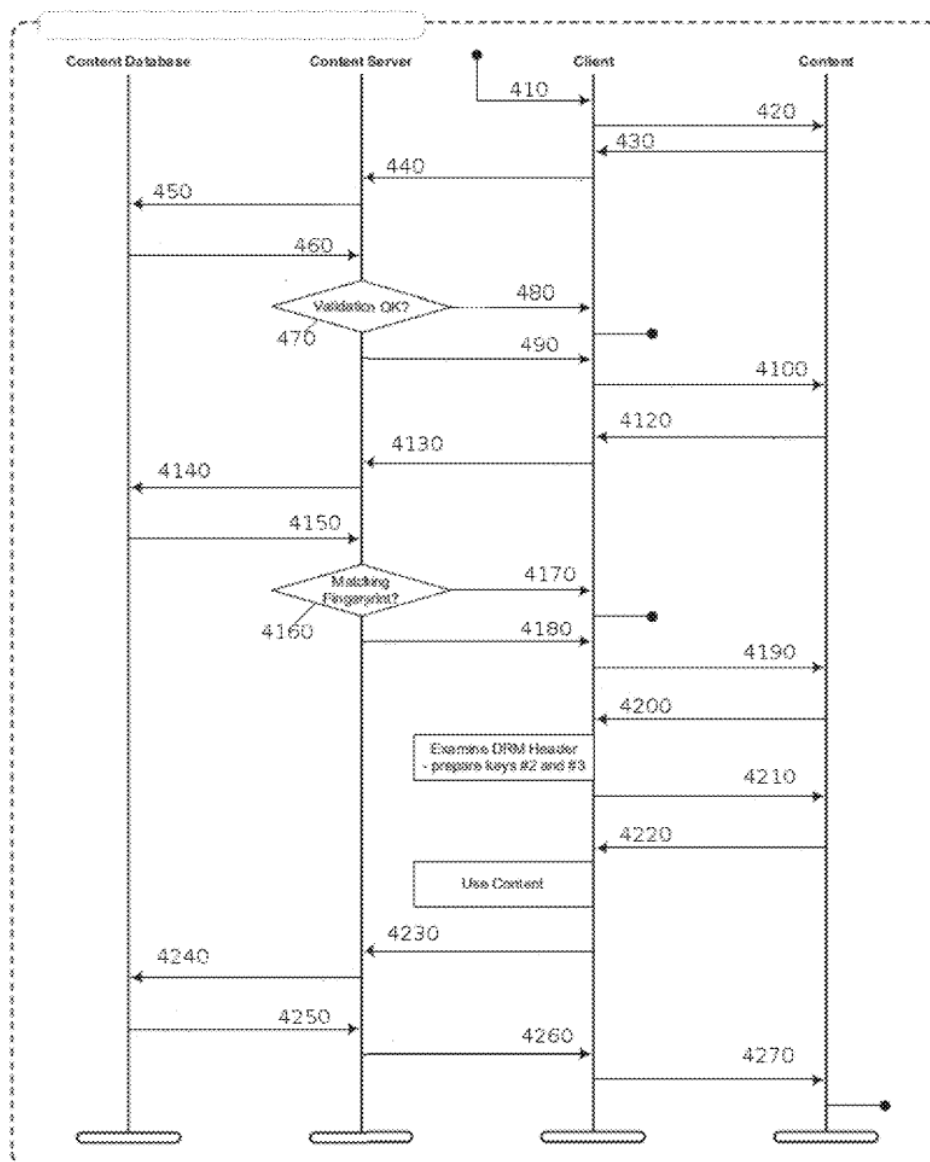


FIG 1

43. The interrogation module 26 interrogates the media storage device 14 “whether or not the received content identifier and user identifier matches with any combination of the stored user identifiers and content identifiers.” (NF-1001, 6:66-7:2.) The validation module 28 retrieves a first digital rights management key (Key #1) and a header associated with the user identifier in response to a determination that the received content identifier and user identifier matches with at least one combination of the stored user identifiers and content identifiers. (NF-1001, 7:16-21.) The calculation module 32 calculates a time period indicative of time in which the user uses the content.” (NF-1001, 8:40-41.)

44. The '102 patent provides three exemplary methods of providing access to access restricted content to a user. Challenged claim 10 is directed to the “first method” illustrated in Figure 4 (reproduced below). In this method, the client acquires content “before the validation starts.” (NF-1001, 11:1-3.) The first method begins in step 410 and proceeds to step 420 when the client locates content, e.g., by searching with a keyword. (NF-1001, 10:4-7.) In response, the client receives a content identifier in step 430. (NF-1001, 10:9-10.) In step 440, the client transmits a message (e.g., a content request) with the content identifier and the identifier of the client to the content server. (NF-1001, 10:10-12.) The content server then sends a query to the content database including the content identifier and client identifier (step 450). (NF-1001, 10:15-17.)



'102 Patent, Figure 4

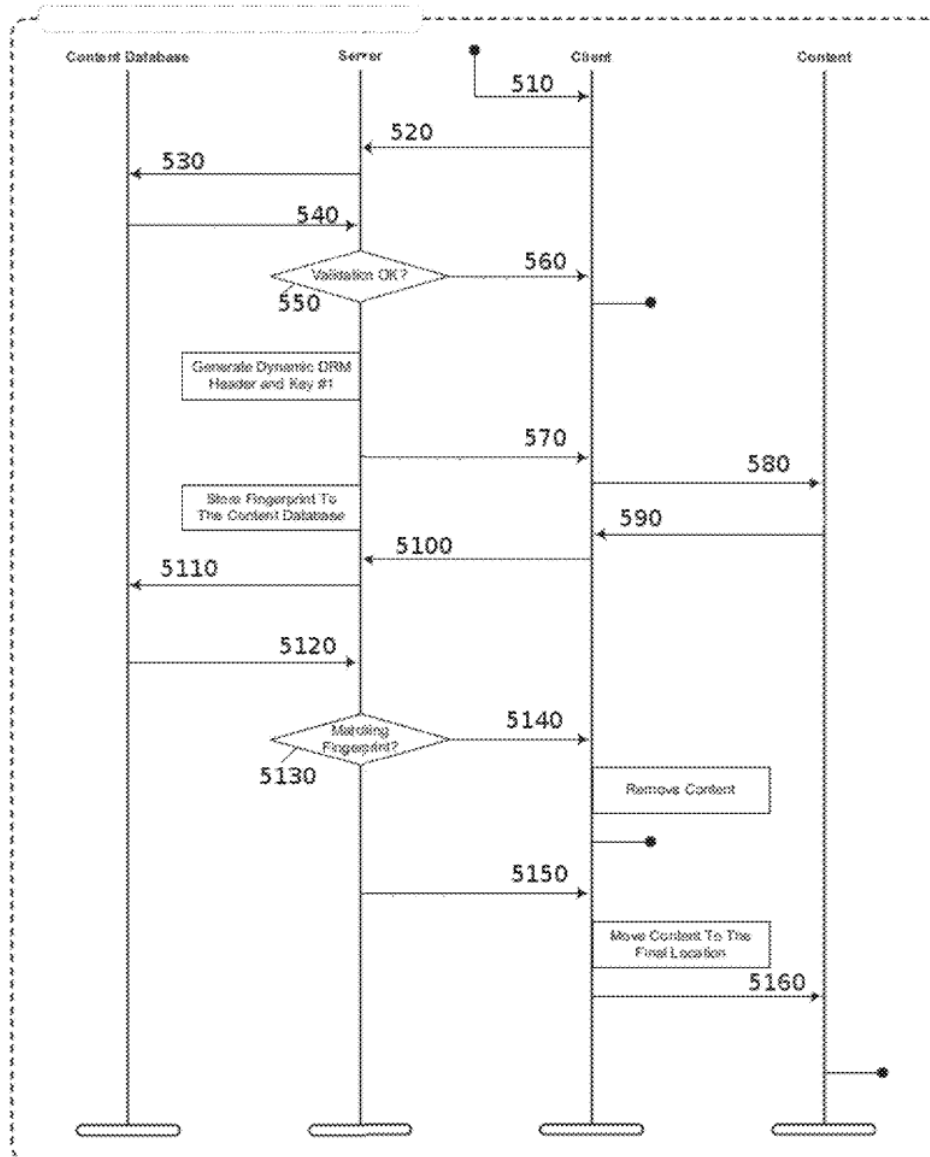
45. The content database returns a validation result comprising a first DRM key (step 460). (NF-1001, 10:18-21.) If validation is successful, the content server transmits the first DRM key to the client (step 490). (NF-1001, 10:21-29.) The client then obtains a fingerprint of the content (step 4120) “based at least in part on the first DRM key.” (NF-1001, 10:30-35.) The client then “transmit[s] the

fingerprint to the content server, optionally with the content identifier” (step 4130). (NF-1001, 10:35-37.) The content server then queries the content database for the content fingerprint (step 4140). (NF-1001, 10:38-39.) The server then “compare[s] the fingerprints” (step 4160) and if the fingerprints match, “the client is provided with a positive validation result” (step 4180). (NF-1001, 10:42-47.)

46. In response to a positive validation result, the client “accesses the content to retrieve a DRM header” (step 4190). (NF-1001, 10:50-52.) Using the DRM header “the client may be enabled to prepare second and third DRM keys, and, optionally, to apply at least one of the second and third DRM keys” (step 4210) to retrieve payload of the content (step 4220). (NF-1001, 10:53-57.) The client then informs the server that the client used the payload of the content. (NF-1001, 10:58-60.) With the first method, “the client has an on-line connection with the server” and “the client has acquired the content before validation starts.” (NF-1001, 11:1-3.)

47. Figure 5 (reproduced below) is a flowchart of a second method for accessing content. This method does not correspond to either of the challenged claims 10 or 11. In this method, the “client requests content from the server” (step 520) which may include the content identifier and client identifier. (NF-1001, 11:6-10.) The server then queries the content database (530) which determines “whether the client should be granted access to the content.” (NF-1001, 11:10-13.) If

validation was successful, “the server generates a DRM header, for example a dynamic DRM header, and a first DRM key.” (NF-1001, 11:14-19.) The server then “encrypts the content and streams it to the client, as well as calculates a content fingerprint” (570). (NF-1001, 11:19-21.)



'102 Patent, Figure 5

48. The client receives the content (580) and “obtains from the content a content fingerprint, which is sent along with the content identifier to the server” (5100). (NF-1001, 11:22-25.) The server then “queries the content database for a content fingerprint of the content.” (NF-1001, 11:26-28.) If the fingerprints match, the client is informed (5150) and the client “validate[s] the content” in step 5160. (NF-1001, 11:34-40.) With the second method, “the client has an on-line connection to the server for receiving the streamed content” and “the client has been registered to the server before the streaming is started.” (NF-1001, 11:41-45.)

49. Figure 6 (reproduced below) is an exemplary flowchart of a third method. The third method does not correspond to challenged claim 10 or 11. In this method, the content accessor (e.g., a client) “requests content from a local provider with a content identifier comprised in the request message” (620). (NF-1001, 11:50-53.) The local provider “locates the content using the content identifier.” (NF-1001, 11:53-55.) If the content exists, the “local provider generates a first DRM key and obtains a DRM header.” (NF-1001, 11:59-60.) The “DRM is verified” (630) and if successful, “the content accessor is granted access to the content” (680). (NF-1001, 11:60-67.) With this method, “the client is able to use the content without leaving it in an unprotected state”, “the content is provided in a format that cannot be stored for later access”, and “the content DRM is accessed only when the content needs to be shown or played.” (NF-1001, 12:1-8.) In other

words, the content is downloaded when needed from the network and not stored at the client device in any format.

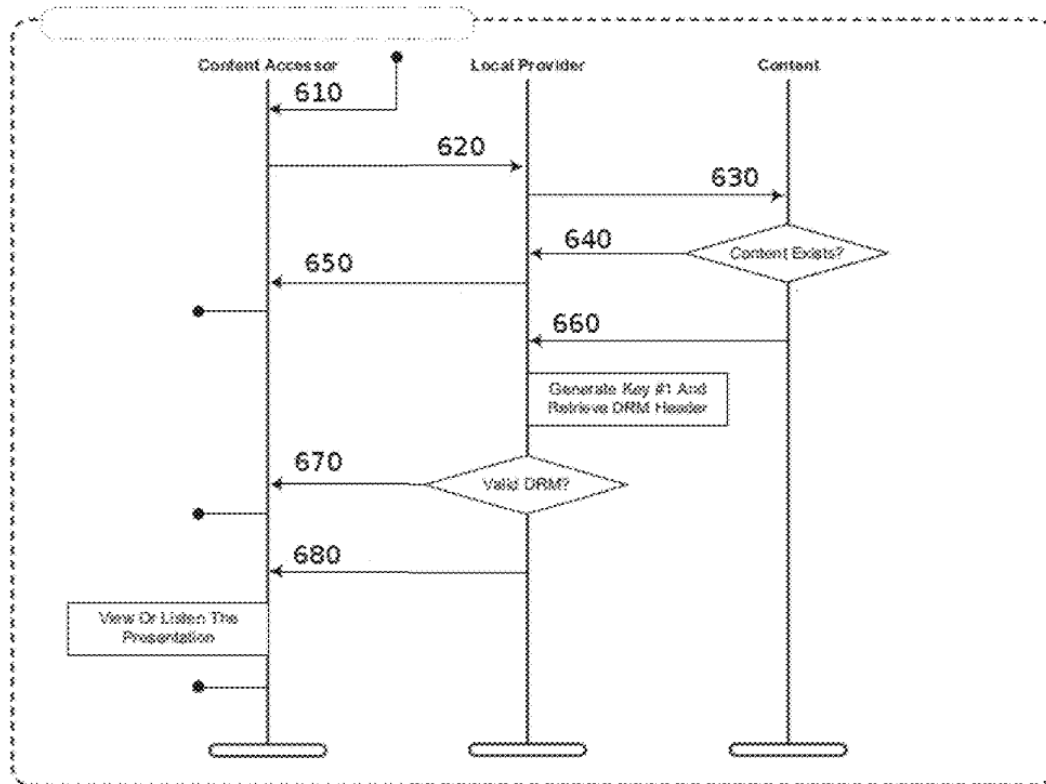


FIGURE 6

'102 Patent, Figure 6

C. Prosecution History

50. The application that became the '102 patent was filed on January 8, 2015. Over the next five years, the Examiner issued multiple rejections (three non-final rejections and two final rejections). In the last rejection made by the Examiner during prosecution, the Examiner found the following claim (which corresponds to limitations of issued claim 10) to be unpatentable over the prior art:

A method, comprising:

obtaining an access restricted content from at least one of a content database and a content providing server;

obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;

deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,

causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and

deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key, wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and

wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key.

(NF-1002, 364-368.)

51. To overcome the rejection, Patent Owner amended this independent claim to recite “wherein the content is usable without being in an unprotected state.” (NF-1002, 393.) Based on this amendment, the Examiner subsequently allowed the claims. (NF-1002, 411.) I note that the ’102 patent provides no explanation or description of this limitation. The closest disclosure relates to the unclaimed embodiment of Figure 6 described above in which the content is maintained in the network and not stored at the client device in any format.

D. Level of Ordinary Skill in the Art

52. I understand that certain issues relating to the validity of the ’102 patent must be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a “person of ordinary skill in the art” or “POSITA” that someone would have had at the time the alleged invention as claimed was made. In §IV.B, I provided an overview of the ’102 patent. In deciding the level of ordinary skill, I have considered the following factors, which I have been informed are relevant to the determination of the level of ordinary skill in the art:

- the levels of education and experience of persons working in the field;
- the types of problems encountered in the art;
- the prior art solutions to these problems;
- the rapidity with which innovations are made; and
- the sophistication of the technology

53. In my opinion, a person having ordinary skill in the art (“POSITA”) at the time of the alleged invention of the challenged claims would have had a bachelor’s degree in computer science or computer engineering and two to four years of experience in digital rights management and/or data security. Significantly more practical experience could also qualify one not having the aforementioned education as a person of ordinary skill in the art while, conversely, a higher level of education could offset a lesser amount of experience.

E. Claim Construction

54. I understand that the Patent Office applies the claim construction standard used in district courts which seeks to give claim terms their plain and ordinary meaning to a person of ordinary skill in the art at the time of the claimed invention. I also understand that if the patent applicant gave a term a special meaning in the specification or during prosecution, then the special meaning should be used. My analysis uses the plain and ordinary meaning to each of the claim terms with the exception of terms which I discuss below.

1. “*Fingerprint*”

55. The term “*fingerprint*” is recited the first time in limitation [10C] which recites “*deriving, using the first digital rights management key, from the access restrict content a fingerprint of the access restricted content.*” A “*fingerprint*” should be construed as “a bit string, derived (or computed) directly from the content, that uniquely represents the content.” The specification does not define the term “*fingerprint*” or provide any details regarding how the “*fingerprint*” is obtained. The term “*fingerprint*” is well-understood in data security field.

56. The term fingerprint would be understood to a layperson as a “unique or distinctive pattern that presents unambiguous evidence of a specific person, substance, disease, etc.” (NF-1012, Webster’s Encyclopedic Unabridged Dictionary of the English Language, 720.) The use of the term “*fingerprint*” in the ’102 patent and field of data security is similar. The “*fingerprint*” of a message or data is a string of bits that uniquely represent the message or data. Digital fingerprints are typically derived or computed using a hash function. For example, Downs explains that “[b]ecause of the properties of the one-way hash functions, one can think of a message digest as a **fingerprint** of the message.” (NF-1005, Downs, 14:13-14.) Walmsley discloses that the “primary application for hash functions is in the reduction of an input message into a digital ‘**fingerprint**’ before the application of a digital signature algorithm.” (NF-1008, Walmsley, 10:3-5.)

57. In the co-pending District Court litigation, the Court found the term “*fingerprint*” means “a unique representation of the content derived directly from the content.” (NF-1013, Markman Order, 14.) The Court’s construction is consistent with Petitioner’s construction because “a bit string, derived (or computed) directly from the content, that uniquely represents the content” is a “unique representation of the content derived directly from the content.”

2. Order of Steps

58. The explicit language of claim 10 imposes the ordering of at least steps [10B]-[10G] which I have reproduced below.

[10B] *obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;*

[10C] *deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,*

[10D] *causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and*

[10E] *deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key,*

[10F] *wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content*

[10G] *wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key*

59. In limitation [10B], the “*first digital rights management key*” is obtained. This key is used in limitation [10C] to “*deriv[e] ... from the access restricted content a fingerprint ...*.” The “*fingerprint*” derived in limitation [10C] is “*validate[d]*” by the “*content proving server*” in limitation [10D]. If that validation is successful, “*the access restricted content*” and “*information describing encryption properties*” is accessed. In limitation [10E], “*a second and third digital rights management key*” are “*derived.*” A POSITA would understand that these are derived using the “*information describing encryption properties of the access restricted content*” accessed in limitation [10D]. Finally, “*the second and third digital rights management keys*” derived in limitation [10E] are “*applied to retrieve the payload of the access restricted content*” in limitation [10F] and the “*at least one of the second or third digital rights management key is used to encrypt the other key ...*” in limitation [10G].

60. This interpretation is consistent with the first method described in the specification that I discussed in the overview of the '102 patent. In this method, the client first obtains a fingerprint using the first DRM key and “transmit[s] the fingerprint to the content server, optionally with the content identifier.” (NF-1001, '102 patent, 10:35-37.) The content server then “compare[s] the fingerprints” and if the fingerprints match, “the client is provided with a positive validation result” (step 4180). (NF-1001, '102 patent, 10:42-47.) In response to a positive validation result, the client “accesses the content to retrieve a DRM header” (step 4190). (NF-1001, '102 patent, 10:48-52.) Using the DRM header “the client may be enabled to prepare second and third DRM keys, and, optionally, to apply at least one of the second and third DRM keys” (step 4210) to retrieve payload of the content (step 4220). (NF-1001, '102 patent, 10:53-57.)

61. In the co-pending District Court litigation, the Court adopted the construction for the ordering of step that “[t]he DRM Keys must be obtained or derived before restricted content is obtained” and “the first DRM key must be obtained and fingerprint validated before the second and third DRM keys are derived.” (NF-1013, Markman Order, 13.) This construction reflects the order of steps of Petitioner’s construction that I discussed above.

V. GROUND 1: Claim 10 is Obvious Over Downs.

A. Overview of Downs

62. Downs relates “to a system and related tools for the secure delivery and rights management of digital assets, such as print media, films, games, and music over global communications networks such as the Internet and the World Wide Web.” (NF-1005, Downs, 1:52-57.) The system is referred to as the Secure Digital Content Electronic Distribution System. Rights management “is implemented through a set of functions distributed among the operating components of the system.” (NF-1005, Downs, 6:66-7:2.) One primary function of rights management is “licensing authorization and control so that content is unlocked only by authorized intermediate or End-User(s) that have secured a license.” (NF-1005, Downs, 7:2-5.)

63. Down’s Secure Digital Content Electronic Distribution System “is a technical platform that encompasses the technology, specifications, tools, and software needed for the secure delivery and rights management of Digital Content and digital content-related content to an end-user, client device.” (NF-1005, Downs, 6:37-41.) The platform “specifies how Digital Content is prepared, securely distributed through point-to-point and broadcast infrastructures (such as cable, Internet, satellite, and wireless) licensed to End-User Device(s), and protected against unauthorized copying or playing. In addition, the architecture of

the technical platform allows for the integration and migration of various technologies such as watermarking, compression/encoding, encryption, and other security algorithms as they evolve over time.” (NF-1005, Downs, 6:49-56.)

64. The system “enables the secure delivery of high-quality, electronic copies of Content 113 to End-User Device(s) 109, whether consumer or business, and to regulate and track usage of the Content 113.” (NF-1005, Downs, 12:8-12.) The system “could be deployed in a variety of consumer and business-to-business services using both new and existing distribution channels.” (NF-1005, Downs, 12:12-15.) “Models such as wholesale or retail purchase, pay-per-listen usage, subscription services, copy/no-copy restrictions, or redistribution could be implemented through the rights management” features. (NF-1005, Downs, 12:18-21.)

1. Downs’ System

65. Figure 6 is a block diagram illustrating the functional elements of Downs’ Secure Digital Content Electronic Distribution system. The system “encompasses several business elements that comprise an end-to-end solution, including: Content Provider(s) 101 or the proprietors of the Digital Content [shaded yellow], Electronic Digital Content Store(s) 103 [shaded blue], Intermediate Market Partners (not shown), Clearinghouse(s) 105 [shaded orange],

Content Hosting Site 111 [shaded green], Transmission Infrastructures 107, and End-User Device(s) 109 [shaded purple].” (NF-1005, Downs, 8:55-65.)

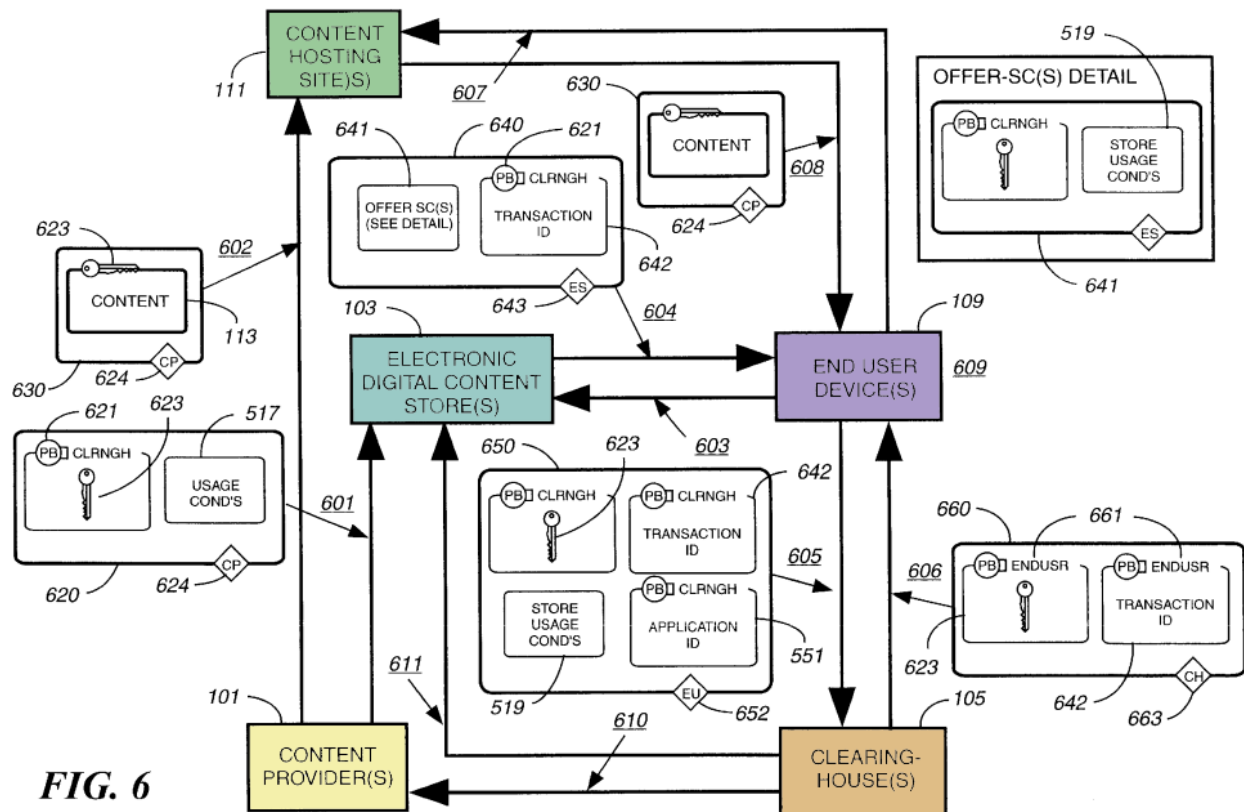


FIG. 6

Downs, Annotated Figure 6

66. In Downs, “Content Provider(s) 101 [shaded yellow] or content proprietor(s) are owners of original Content 113 and/or distributors authorized to package independent Content 113 for further distribution.” (NF-1005, Downs, 9:5-7.) Example Content Providers include “Sony, Time-Warner, MTV, IBM, Microsoft, Turner, Fox, and others.” (NF-1005, Downs, 9:12-14.) The Content Provider prepares its “Content 113 and related data for distribution.” (NF-1005,

Downs, 9:15-18.) The “data related to the Content 113” is referred to as metadata. (NF-1005, Downs, 9:21-23.) “As an example, metadata for a song may be a song title or song credits.” (NF-1005, Downs, 9:24-25.) The Content 113 in this example contains the sound recording. (NF-1005, Downs, 9:26-27.)

67. The Content Provider 101 packs “encrypted Content 113, digital content-related data or metadata, and encrypted keys” in a secure containers (SCs). (NF-1005, Downs, 9:48-51.) The SCs are “stored in a content hosting site [shaded green] and/or promotional web site for electronic distribution.” (NF-1005, Downs, 9:50-51.) “The content hosting site can reside at the Content Provider(s) 101 or in multiple locations, including Electronic Digital Content Store(s) 103 and Intermediate Market Partners (not shown) facilities.” (NF-1005, Downs, 9:52-55.)

68. Electronic Digital Content Stores 103 [shaded blue] “market the Content 113 through a wide variety of services or applications, such as Content 113 theme programming or electronic merchandising of Content 113.” (NF-1005, Downs, 9:62-65.) Electronic Digital Content Stores 103 “aggregate information from the Content Provider(s) 101, pack content and metadata in additional SCs, and deliver those SCs to consumers or businesses as part of a service or application.” (NF-1005, Downs, 10:6-10.) The Electronic Digital Content Store “may elect to host the SCs containing the Digital Content at its local site and/or utilize the hosting and

distribution facilities of another Content hosting site.” (NF-1005, Downs, 10:26-29.)

69. Clearinghouse 105 [shaded orange] “provides the licensing authorization and record keeping for all transactions that relate to the sale and/or permitted use of the Content 113 encrypted in a SC.” (NF-1005, Downs, 10:50-53.)

Clearinghouse 105 “keeps a record of all transactions and can report them to responsible parties, such as Electronic Digital Content Store(s) 103 and Content Provider(s) 101, on an immediate, periodic, or restricted basis.” (NF-1005, Downs, 11:1-5.) The reporting is a means by which a Content Provider 101 “can be informed of the sale of Content 113 and the Electronic Digital Content Store(s) 103 can obtain an audit trail of electronic delivery to their customers.” (NF-1005, Downs, 11:5-8.)

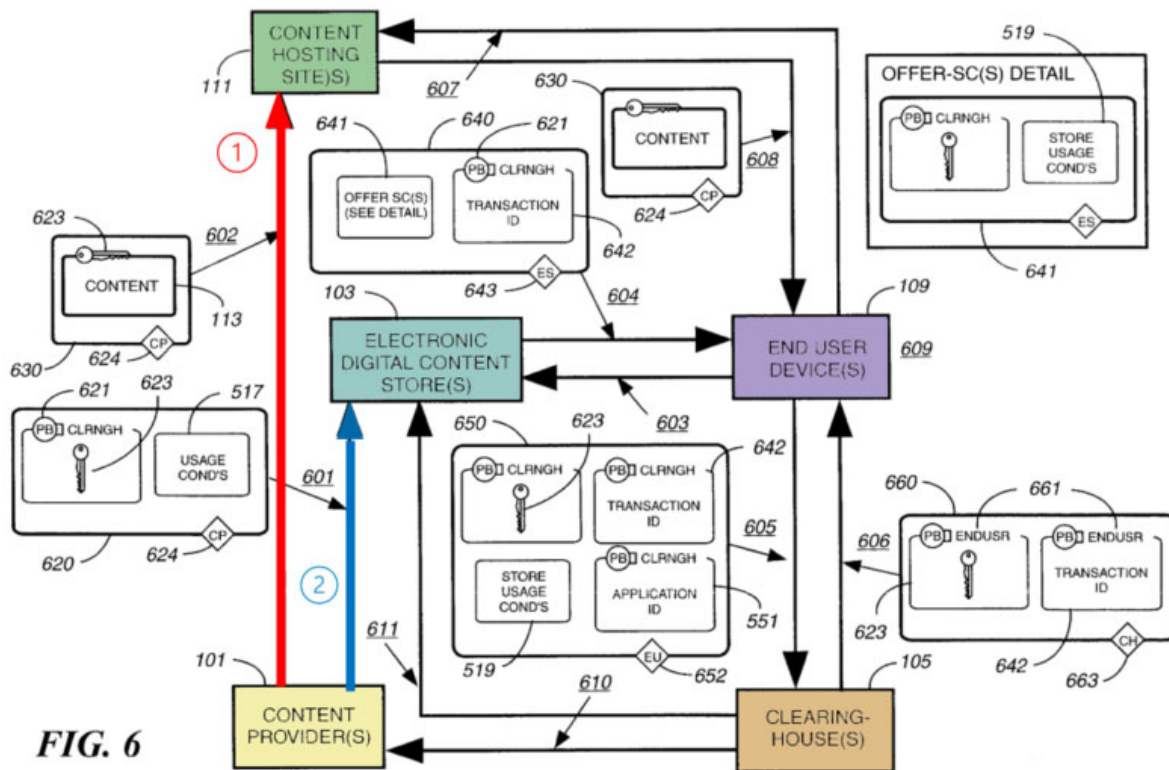
70. An End-User Device 109 [shaded purple] “can be any player device that contains an End-User Player Application 195” compliant with the specifications of the system. “These devices may include PCS, set top boxes (IRDs), and Internet appliances.” (NF-1005, Downs, 11:30-34.) “In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management” in the End-User Device. (NF-1005, Downs, 11:36-40.) The End-User Device 109 “manages the download and storage of the SCs containing the Digital Content; requests and manages receipt of the

encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted.” (NF-1005, Downs, 11:40-48.)

2. Overview of Distribution Flow

71. In operation, the Content Provider 101 “encrypts the Content 113 using an encryption symmetric key locally generated, and encrypts the Symmetric Key 623 using the Clearinghouse’s 105 public key 621.” (NF-1005, Downs, 23:30-33.) Content Provider 101 packs “encrypted Content 113, digital content-related data or metadata, and encrypted keys” in secure containers (SCs). (NF-1005, Downs, 9:48-51.) For example, the encrypted symmetric key, metadata and other information about the Content 113 are “packed into a Metadata SC” and the encrypted content 113 and metadata are packed into a Content SC. (NF-1005, Downs, col. 18 (steps 126-127; 23:33-37).) “There is one Metadata SC(s) 620 and one Content SC(s) 630 for every Content 113 object.” (NF-1005, Downs, 23:37-39.) The Content SC is sent to the Content Hosting Site 111 (red arrow labeled 1 in Figure 6 below) which can reside at either Content Provider 101, Clearinghouse 105 or a special location dedicated for Content Hosting. (NF-1005, Downs, col. 18 (step 129; 23:44-45).) The Metadata SC 620 associated with the content is distributed to “one or more

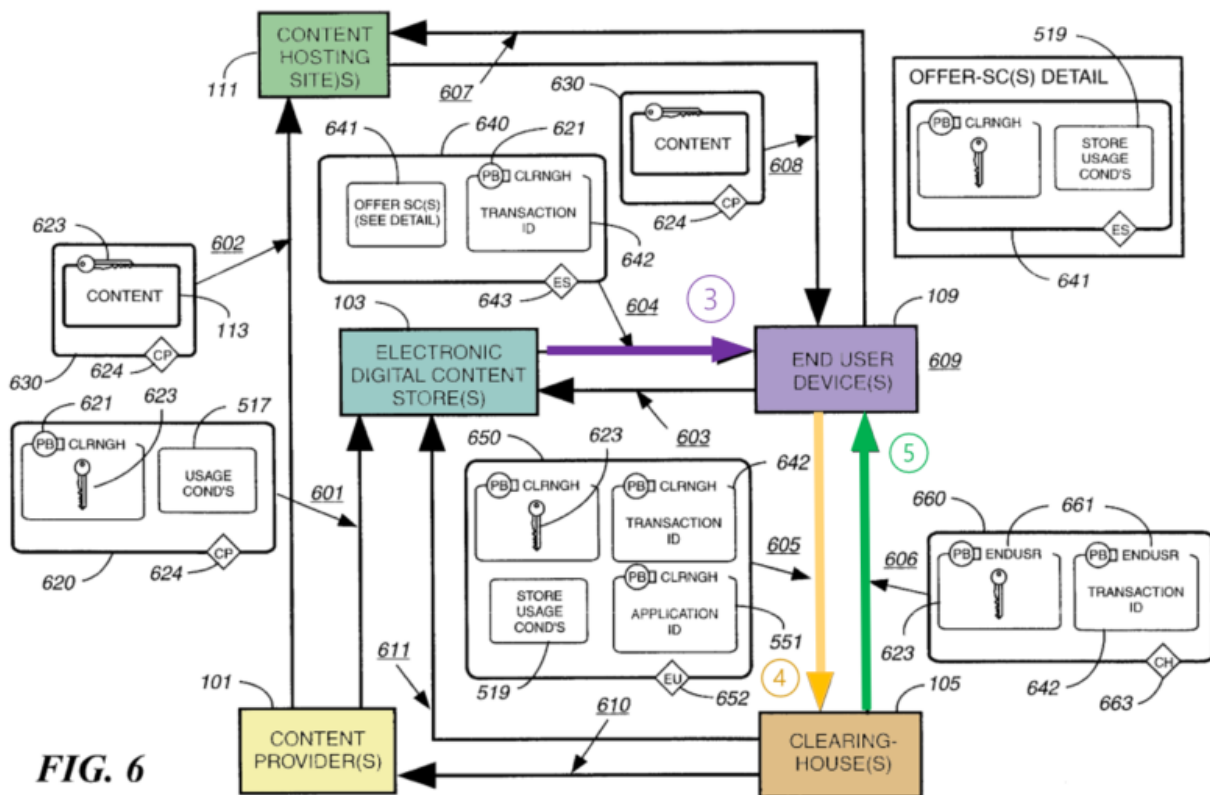
Electronic Digital Content Store(s) 103” (blue arrow labeled 2). (NF-1005, Downs, 23:42-44.)



Downs, Annotated Figure 6

72. The Electronic Digital Content Store 103 creates an Offer SC 641 to offer the content to End-Users. (NF-1005, Downs, 23:45-46.) After completion of the purchase of content by the End-User Device, “the Electronic Digital Content Store(s) 103 creates and transfers to the End-User Device(s) 109 a Transaction SC(s) 640.” (NF-1005, Downs, 23:57-61.) The Transaction SC 640 “includes a unique Transaction ID 535, the purchaser’s name (i.e., End-User(s)) (not shown), the Public Key 661 of the End-User Device(s) 109, and the Offer SC(s) 641

associated with the purchased Content 113” (purple arrow labeled 3 in Figure 6 below). (NF-1005, Downs, 23:62-65.)



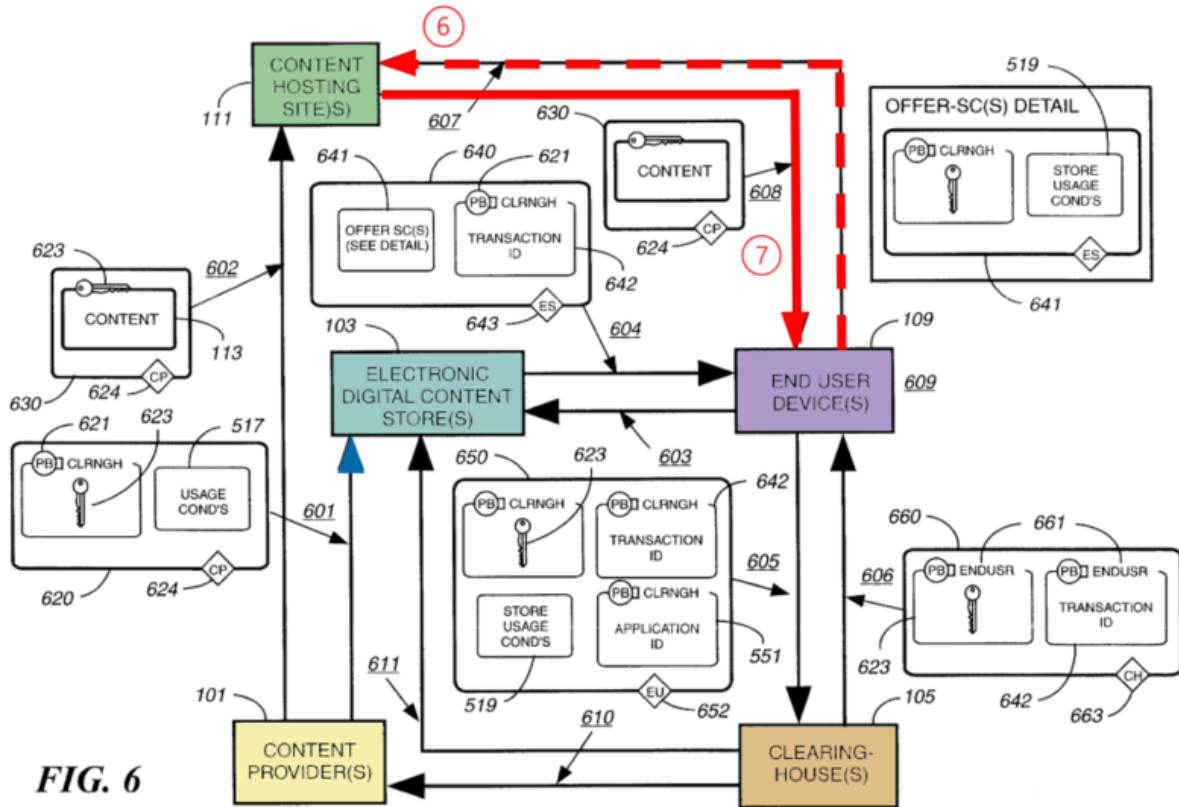
Downs, Annotated Figure 6

73. Upon receipt of the Transaction SC 640 (and the included Offer SC), the End-User Device 109 “solicits license authorization from the Clearinghouse(s) 105 by means of an Order SC(s) 650” (yellow arrow labeled 4 above). (NF-1005, Downs, 24:5-9.) The Order SC “includes the encrypted Symmetric Key 623 and Store Usage Conditions 519 from the Offer SC(s) 641, the encrypted Transaction Data 642 from the Transaction SC(s) 640, and the encrypted Application ID 551 from the End-User Device(s) 109.” (NF-1005, Downs, 24:9-14.) The Order SC 650

“is signed with a Digital Signature 652 of the End-User Device(s) 109.” (NF-1005, Downs, 24:14-16.)

74. Upon receipt of the Order SC 650 from the End-User Device, the Clearinghouse 105 verifies, for example, that the Order SC 650 has not been altered and the Transaction Data 642 and Symmetric Key 623 are complete and authentic. (NF-1005, Downs, 24:17-32.) If the verifications are successful, Clearinghouse 105 “decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the License SC(s) 660 to the End-User Device(s) 109.” (NF-1005, Downs, 24:34-37.) The License SC “carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device(s) 109” (green arrow labeled 5). (NF-1005, Downs, 24:37-40.)

75. Upon receipt of the License SC 660, End-User Device 109 “decrypts the Symmetric Key 623 and the Transaction Data 642 previously received from the Clearinghouse(s) 105 and requests the Content SC(s) 630 (step 607) from a Content Hosting Site(s) 111” (red dashed arrow labeled 6 below). (NF-1005, Downs, 24:48-52.) “Upon arrival of the Content SC(s) 630 (step 608) [red arrow labeled 7], the End-User Device(s) 109 decrypts the Content 113 using the Symmetric Key 623 (step 609), and passes the Content 113 and the Transaction Data 642 to the other layers for license watermarking, copy/play coding, scrambling, and further Content 113 processing.” (NF-1005, Downs, 24:52-57.)



Downs, Annotated Figure 6

B. Independent Claim 10

76. Downs discloses or suggests the preamble and each of the limitations of claim 10. For ease of discussion, I reproduce the text of independent claim 10 below with labels.

[10P] *A method, comprising:*

[10A] *obtaining an access restricted content from at least one of a content database and a content providing server;*

[10B] *obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;*

[10C] *deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,*

[10D] *causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and*

[10E] *deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key,*

[10F] *wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and*

[10G] *wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key,*

[10H] *wherein the content is usable without being in an unprotected state.*

1. Preamble [10P]

77. Downs discloses a “method and apparatus of securely providing data to a user's system.” (NF-1005, Downs, Abstract.) The data is encrypted and is “decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key.” (*Id.*) Downs therefore discloses a “*method*” [10P].

2. “*Obtaining an access restricted content*” [10A].

78. Content Provider 101 (shaded yellow below) “is the digital content label or entity who owns the rights to the Content 113.” (NF-1005, Downs, 48:29-31.) The Content Provider “use[s] tools provided as part of the Secure Digital Content Electronic Distribution System 100 in order to prepare their Content 113 and related data for distribution.” (NF-1005, Downs, 9:15-18.) Related content data includes metadata which is “data related to the Content 113.” (NF-1005, Downs, 9:21-24.) For example, metadata for a song is the song title or credits but not the sound recording itself. (NF-1005, Downs, 9:24-26.) In Downs, the Content Provider 101 in annotated Figure 6 below “encrypts the Content 113 using an encryption symmetric key locally generated.” (NF-1005, Downs, 23:30-31.) The content and its associated metadata are “*access restricted content*.”

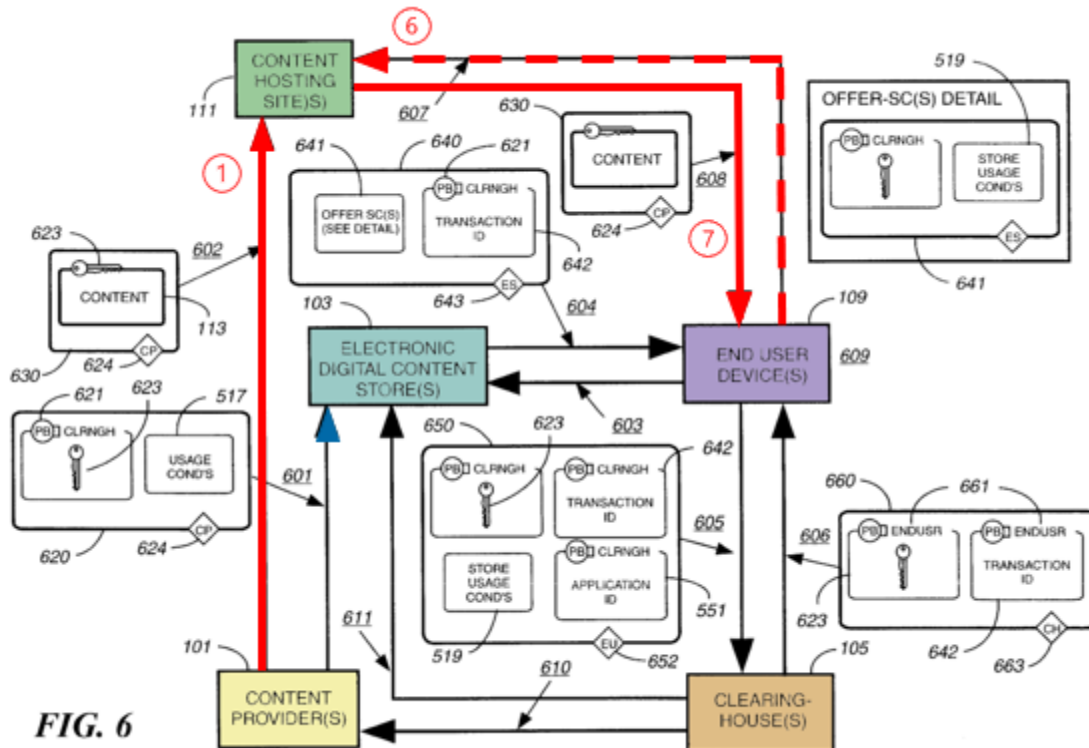


FIG. 6

Downs, Annotated Figure 6

79. As I discussed in further detail in §V.A, the encrypted content is packed with metadata into a Content SC and distributed to a Content Hosting Site 111 (indicated by the red arrow labeled 1 in Figure 6 above). After the End-User Device (shaded purple) receives a License SC from Clearinghouse 105, the End-User Device requests the licensed content from the Content Hosting Site 111 (indicated by the dashed red arrow labeled 6) which then provides the requested content to the End-User Device (indicated by the solid red arrow labeled 7). (NF-1005, Downs, 24:48-57.) Content Hosting Site 111 (shaded green) is a “*content providing server*” because it serves content to requesting End-User Devices. Thus,

End-User Device 109 “*obtain[s] an access restricted content from at least one of a content database and a content proving server*” [10A].

3. “*Fingerprint*” Limitations

80. Independent claim 10 recites the following three limitations directed to the “*fingerprint of the access restricted content.*” As I detail in this section, Downs teaches or suggests these limitations.

[10B] *obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;*

[10C] *deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based¹ at least in part on the first digital rights management key;*

¹ Claim 10 lacks a clear antecedent basis for the phrase “*the obtaining is based at least in part on the first digital rights management key.*” The phrase could apply to either the “*obtaining an access restricted content*” of limitation [10A] or the “*deriving*” of limitation [10C]. Solely for purposes of this IPR, I have been instructed to assume that “*obtaining is based ...*” applies to the “*deriving*” of limitation [10C] based on the parallel language of claim 1. I note that this position is consistent with the findings of the Court in the co-pending District Court

[10D] *causing the content providing server to validate the fingerprint*

81. End-User device 109 “initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111.” (NF-1005, Downs, 69:40-42.) The License SC includes the “Content ID” which is “a unique ID assigned to a Content 113 item.” (See NF-1005, Downs, 37:26-38:20; 29:30-31.) Before providing the requested Content SC to the End-User, a database of License SC IDs is checked to ensure the End-User Device “only makes one request for each piece of Content 113 purchased.” (NF-1005, Downs, 70:4-10.) Although not explicit, a POSITA would understand that the hosting device uses an identifier associated with the end-user device to assess whether only one request for the content has been made. For example, a POSITA would have understood the Content Hosting Site maintains a data structure listing end user device and content ID pairs for requested content. A pair is added to the data structure when a new request is received. A subsequent request for the same content by the same End-User device would therefore be denied because the end user device-Content ID pair exists in the data structure. The request to the Content Hosting Site by the

litigation which found that “[i]t is thus clear that ‘deriving,’ id. at 14:8, is the antecedent basis for the contested term.” (See NF-1013, 10.)

End-User Device is therefore “*a query*” that “*compris[es] the content identifier and an identifier associated with the user.*”

82. In Downs, a Content Hosting Router “resides in the Content Hosting Site(s) 111 and receives all requests from End-User(s) wanting to download Content 113.” (NF-1005, Downs, 70:18-20.) The Router “performs the validation checks on the End-User(s) request to ensure they indeed bought the Content 113.” (NF-1005, Downs, 70:20-22.) The Content Hosting Site maintains a database having “the status of the Secondary Content Sites” including “what Content 113 is on them and there [sic] current status.” (NF-1005, Downs, 70:22-24.) The Content Hosting Site receiving the End-User request for content is referred to by Downs as the “primary content site.” (NF-1005, Downs, 69:51-54.) The primary content site makes the decision of which secondary site should be used to access the requested content. (See NF-1005, Downs, 69:51-54.) Although not explicit, a POSITA would understand from Downs that the primary content site (Content Hosting Site 111) retrieves the requested Content SC from the appropriate secondary content site for delivery to the End User.

83. The contents of the Content SC (reproduced below) include the Certificate for the Content Provider. The certificate “includes the public key, the name of the person or entity, an expiration date, the name of the certification authority, and other information.” (NF-1005, Downs, 14:23-25.) The Content

Provider's public key and its associated private key (the Content Provider's asymmetric key pair) are the "*first digital rights management key.*" A POSITA would understand that the Content SC is stored on the secondary content site in a content database because prior to January 2014 a database was and remains a common repository for storing data. (See, e.g., NF-1011, 80 (explaining that the content server has a content repository which is a database containing content).) Thus, when the primary content site (Content Hosting Site 111) requests the Content SC from the secondary content site, it obtains the Content SC which includes the "*first digital rights management key from a content database*" (content provider public key included in the certificate). Thus, Downs discloses "*obtaining a first digital rights management key from a content database.*" As I discussed above, the request for the Content SC is based on the query received from the End-User device including the "*content identifier and an identifier associated with the user.*" Downs therefore discloses the "*obtaining is based in part on a query, the query comprising the content identifier and an identifier associated with the user*" [10B].

Parts	BOM	
	Part Exists	Digest
	SC(s) Version	
	SC(s) ID	
	SC(s) Type	
	SC(s) Publisher	
	Date	
	Expiration Date	
	Clearinghouse(s) 105 URL	
	Digest Algorithm ID	
	Digital Signature Alg ID	
Content ID	Yes	Yes
Encrypted Content	Yes	Yes
Encrypted Metadata	Yes	Yes
Metadata	Yes	Yes
Certificate(s)	Yes	No
	Digital Signature	

Downs, Content SC

84. The Content SC (reproduced above) also includes the encrypted content and a digest of the encrypted content. Specifically, the Content Provider “runs the encrypted content through a hash algorithm to produce the content digest.” (NF-1005, Downs, 15:65-66.) In Downs, a “one-way hash digest is used to calculate a message digest.” (NF-1005, Downs, 14:6-7.) The hash algorithm takes an input message “and converts it into a fixed length string, the message digest.” (NF-1005, Downs, 14:7-9.) “Because of the properties of the one-way hash functions, one can think of a message digest as a **fingerprint** of the message.” (NF-1005, Downs, 14:13-14.) The Content Provider also creates a digest for the entire Content SC by concatenating the individual digests associated with Content SC (encrypted content digest, encrypted metadata digest, and metadata digest). (NF-1005, Downs, 16:8-

10.) The Content SC digest is encrypted with the **Content Provider’s private key** [the recited “*first digital rights management key*”] to produce the digital signature for the SC (306). (NF-1005, Downs, 16:11-13.) The digital signature is “*a fingerprint of the access restricted content*” that is “*derived, using the first digital rights management key, from the access restricted content, wherein the obtaining [deriving] is based at least on the first digital rights management key*” [10C]. The digital signature is a bit string and is a unique representation of the content derived directly from the content.

85. Upon receipt of the Content SC, the Content Hosting Site (primary content site) verifies the integrity of the Content SC. As explained by Downs, “recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests.” (NF-1005, Downs, 14:3-5; *see also*, NF-1005, Downs, 25:14-18 (“Parties receiving the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts”).) Specifically, the Content Hosting Site “decrypts the SC(s) digital signature” using the Content Provider’s public key. (NF-1005, Downs, col. 16 (step 410).) The recipient runs the concatenation of the received content digest through the same hash algorithm used by the Content Provider to compute the SC digest. (NF-1005, Downs, col. 16 (step 411).) The Content Hosting Site then compares the computed Content SC digest with the one

recovered from the Content Provider’s digital signature. (NF-1005, Downs, col. 16 (step 412).) “If they are the same, recipient confirms that the received digests have not been altered.” (NF-1005, Downs, col. 16 (step 412).) Thus, the system “*caus[es] the content providing server [Content Hosting Site] to validate the fingerprint*” [10D] in order to verify the integrity of the Content SC received from a secondary hosting site (e.g., that the content has not been altered or replaced).

4. “*Access[ing] Restricted Content*”

86. Independent claim 10 recites the following limitations directed to the “*accessing the access restricted content.*” As I detail in this section, Downs teaches or suggests these limitations.

[10D] ... *if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and*

[10E] *deriving, using the digital rights management header² of the access restricted content, from the access restricted content a second and third digital rights management key,*

² Claim 10 lacks antecedent basis for “*the* digital rights management header.” Solely for purposes of this IPR, Petitioner assumes the claim is intended to recite “*a digital rights management header.*” Petitioner reserves the right to argue indefiniteness of this term in another forum.

[10F] *wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and*

[10G] *wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key*

87. Upon purchase of the content, the Clearinghouse provides the License SC to the End-User Device as I discussed above. As I discussed in the previous section, the End-User Device requests the Content SC from the Content Hosting Site 111 using the License SC. If the integrity of the Content SC is verified by the Content Hosting Site 111 (primary content site), the Content SC is transmitted to the End User Device 109. (See NF-1005, Downs, 70:4-6.) At this point in the process flow, the End-User Device therefore has both the License SC and Content SC associated with the requested content.

88. To play the content received from the primary content site, the End-User Device must access the License SC received from the Clearinghouse. The License SC “provides an End-User Device(s) 109 with everything that is needed to access a Content 113 item.” (NF-1005, Downs, 28:4-5.) The contents of the License SC are provided in the Table below. The License SC 660 “carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 661 of the End-User Device.” (NF-1005, Downs, 24:37-40.) As shown in the Table below, the key description part of the License SC indicates the encryption algorithm used to

encrypt the symmetric key for the content, the symmetric key algorithm, and the identifier of the key used to encrypt the content, metadata, and watermarking instructions. (See, e.g., NF-1005, Downs, 37:26-38:20.) This information is “*information describing the encryption properties of the access restricted content.*”

The End-User Device receives the Content SC only after the fingerprint of the access restricted content has been validated by the Content Hosting Site as I discussed above. Because the End-User Device accesses the License SC to play the content in the received Content SC, the End-User Device “*access[es] ... information describing the encryption properties of the access restricted content*” if the “validation” of the integrity of the Content SC using the message digest (“fingerprint”) is successful. [10D].

Parts	BOM		Key Description Part				
	Part Exists	Digest	Result Name	Encrypt Alg	Key ID/Enc Key	Sym Key Alg	Sym Key ID
[Content URL]			Output Part	RC4	Enc Sym Key	RSA	EU Pub Key
[Metadata URL]			Output Part	RC4	Enc Sym Key	RSA	EU Pub Key
	SC(s) Version						
	SC(s) ID						
	SC(s) Type						
	SC(s) Publisher						
	Date						
	Expiration Date						
	Digest Algorithm ID						
	Digital Signature Alg ID						
Content ID	Yes	Yes					
Order SC(s) ID	Yes	Yes					
Watermarking Instructions	Yes	Yes	Output Part	RC4	Enc Sym Key	RSA	EU Pub Key
Key Description Part	Yes	Yes					
Certificate(s)	Yes	No					
	Digital Signature						

Downs, License SC

89. As shown in the table above, the License SC indicates in the Key Description Part that the symmetric key was encrypted using the “EU Pub Key” which is the public key portion of the End User Device’s asymmetric key pair. The Key Description Part is a header of the License SC which is associated with the access restricted content. For example, the Content URL of the License SC “points to the encrypted Content 113 in the Content SC(s) 630.” (*See, e.g., NF-1005, Downs, 29:19-24; 37:58-60.*) The Content ID of the License SC “defines a unique ID assigned to a Content 113 item.” (NF-1005, Downs, 29:30-33; 37:58-60.) Thus, the Key Description Part is a “*digital rights management header of the access restricted content*” [10E]. From this “*header*” information, the End-User Device “*derives*” the associated private key portion of its asymmetric key pair (public/private keys) to use to decrypt the Symmetric Key. The End-User’s asymmetric key pair is collectively the “*second digital rights management key*” and is derived “*using the digital rights management header of the access restricted content*” [10E].

90. Using the “*second digital rights management key*” and the information concerning the encryption algorithm provided in the License SC header, the End-User device decrypts the Symmetric Key for the Content which is a “*third digital rights management key*.” Thus, the End-User Device also “*deriv[es]*” the “*third digital rights management key*” using the information in the Key Description Part

of the License SC (“*digital rights management header*”). Because the Symmetric Key (“*third digital rights management key*”) is encrypted with the public key portion of the End User Device’s asymmetric key pair (“*second digital rights management key*”), Downs discloses “*at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key*” [10G].

91. The End-User Device then “decrypts the Content 113 using the Symmetric Key 623.” (NF-1005, Downs, 24:54-55.) Through these steps, the End-User Device “*access[es] the access restricted content*” in the Content SC [10D]. In Downs, the private key portion of the End-User’s asymmetric key pair is applied to decrypt the Symmetric Key and the Symmetric Key is applied to decrypt the encrypted content in the Content SC (the recited “*access restricted content*”). Thus, Downs teaches “*the second and third digital rights management keys are applied to retrieve the payload of the access restricted content*” [10F].

92. Claim 10 further recites that the “*content is useable without being in an unprotected state.*” The specification includes a single mention of the state of content. Specifically, the specification indicates “the client is able to use the content without leaving it in an unprotected state” in the third method described in the specification. (See §IV.B.) In this method, the content is maintained in the network and not stored in any format on the client device. Content not “*in an*

unprotected state” is protected content. Therefore, as written, this limitation recites the content is usable when the content is in a protected state (e.g., encrypted). A POSITA would have understood that encrypted (protected) content is not directly useable by the client device. The client device must first decrypt the content. Should PO contend this limitation covers the circumstance where content is stored in encrypted form and then decrypted using a stored decryption key, such a process is (1) not disclosed in the ’102 patent and (2) was extremely well-known for decades prior to the ’102 patent as discussed in both Subramanya and Rosenblatt, for example. (See NF-1010, 31-32; NF-1011, 80-84.)

93. Specifically, after decrypting the Content using the Symmetric Key provided by the Content Provider, the End-User Device “re-encrypt[s] the Content 113 using a random Symmetric Key.” (NF-1005, Downs, 82:20-34.) This key is encrypted and stored in the License database for the End-User Device. (NF-1005, Downs, 82:34-39.) Once the content has been re-encrypted, “it is stored in the Digital Content Library 196.” (NF-1005, Downs, 83:16-17.) When content is accessed, the Player Application “perform[s] a real-time concurrent decryption-decode-playback of the Content 113 without the need to first decrypt the entire file for the Content 113 prior to decode and playback.” (NF-1005, Downs, 82:51-55.) Therefore, in Downs, content is stored in the End-User Device in encrypted form and decrypted in real-time when the content is consumed by a user.

VI. GROUND 2: Claims 10-11 Are Obvious Over DeMello, Schwartz, and Walmsley.

A. Overview of the Combination

1. DeMello

94. DeMello “is directed to a system for processing and delivery of electronic content wherein the content may be protected at multiple levels.” (NF-1006, DeMello, 4:41-43.) The preferred embodiment described in DeMello “is directed to the processing and delivery of electronic books, however, the invention is not limited to electronic books and may include all digital content such as video, audio, software executables, data, etc.” (NF-1006, DeMello, 4:44-49.)

a. Content

95. DeMello provides an infrastructure “which supports the distribution of protected content in a digital rights management (‘DRM’) system.” (NF-1006, DeMello, 1:60-62.) “The primary users of the DRM System are publishers and retailers, who use and/or deploy the DRM System to ensure legitimacy of the content sold as well as copy protection.” (NF-1006, DeMello, 5:8-10.) DeMello’s system “accomplishes its goals by protecting works, while enabling their rightful use by consumers, by supporting various ‘levels’ of protection.” (NF-1006, DeMello, 5:23-26.)

96. At the Level 1, the lowest level of protection, “the content source and/or provider may choose no protection via unsigned and unsealed (clear-text) eBooks

that do not include a license.” (NF-1006, DeMello, 5:26-29.) At Level 2, the content “is ‘source sealed,’ which means that the content has been encrypted and sealed with a key, where the seal is made using a cryptographic hash of the eBook's title's meta-data [] and the key is necessary to decrypt the content.” (NF-1006, DeMello, 5:29-34.) At Level 3, content is “individually sealed” (or “inscribed”). (NF-1006, DeMello, 5:44-45.) “An ‘individually sealed’ title is an eBook whose meta-data includes information related to the legitimate purchaser (e.g., the user's name or credit card number, the transaction ID or receipt number from the purchase transaction, etc.), such that this information is cryptographically bound to the content when the title is sealed.” (NF-1006, DeMello, 5:45-51.)

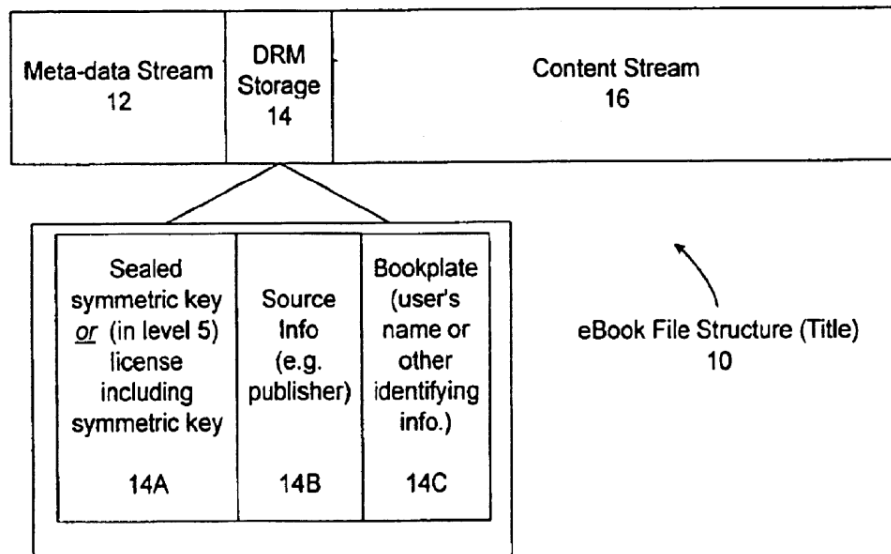
97. At Level 4, content is “source signed.” (NF-1006, DeMello, 5:57-58.) Source signed content “can be authenticated by a ‘reader’” which is a user application that enables the “reading of eBooks on a computing device.” (NF-1006, DeMello, 5:58-61.) “Authenticity may preferably be defined in three varieties: ‘tool signed,’ which guarantees that the eBook title was generated by a trusted conversion and encryption tool; ‘owner signed,’ which is a tool signed eBook that also guarantees the authenticity of the content in the copy (e.g., the owner may be the author or other copyright holder); and ‘provider signed,’ which is a tool signed eBook that attests to the authenticity of its provider (e.g., the publisher or retailer of the content).” (NF-1006, DeMello, 5:63-6:4.) Content can be “both provider

signed and source signed, which facilitates authentication of the distribution channel of the title (e.g., through a signature chain in the copy).” (NF-1006, DeMello, 6:7-10.) Level 5, “fully individualized” or “owner exclusive”, is the “strongest level of protection.” (NF-1006, DeMello, 6:10-11.) “‘Fully individualized’ titles can only be opened by authenticated reader applications that are ‘activated’ for a particular user, thereby protecting against porting of a title from one person’s reader (or readers) to a reader that is not registered to that person.” (NF-1006, DeMello, 6:11-16.) For the reader to open a Level 5 title, “the Reader must be ‘activated’ (i.e., the device on which the reader resides must have an activation certificate for a particular persona, and a secure repository).” (NF-1006, DeMello, 6:16-20.)

98. The exemplary file structure for content is illustrated in Figure 1 below for an exemplary eBook. eBook 10 contains content 16 “that has been encrypted by a key (the ‘content key’), which itself has been encrypted and/or sealed.” (NF-1006, DeMello, 6:39-42.) The “key is a symmetric key 14A that is sealed with a cryptographic hash of metadata 12 or, in the case of level 5 titles, with the public key of the user’s activation certificate.” (NF-1006, DeMello, 6:42-45.) The “key is stored either as a separate stream in a sub-storage section of the eBook file (DRM Storage 14 in the diagram) or, in the case of level 5 titles, in the license.” (NF-1006, DeMello, 6:45-48.) For level 5 titles, “instead of storing the content key as a

separate stream, stream 14A contains a license, which is a construct that defines the rights that the user can exercise upon purchase of the title.” (NF-1006, DeMello, 6:48-53.) The content key “is contained within the license.” (NF-1006, DeMello, 6:52-53.) Also included in DRM storage “are the source stream 14B, which may include the name of the publisher (or other content source), as well as the bookplate stream 14C, which, for individually sealed (level 3 and/or level 5) titles, includes the consumer’s name as provided by the retailer (which may, for example, be obtained as part of the commercial transaction of purchasing an eBook 10, such as from the consumer’s credit card information).” (NF-1006, DeMello, 6:53-60.)

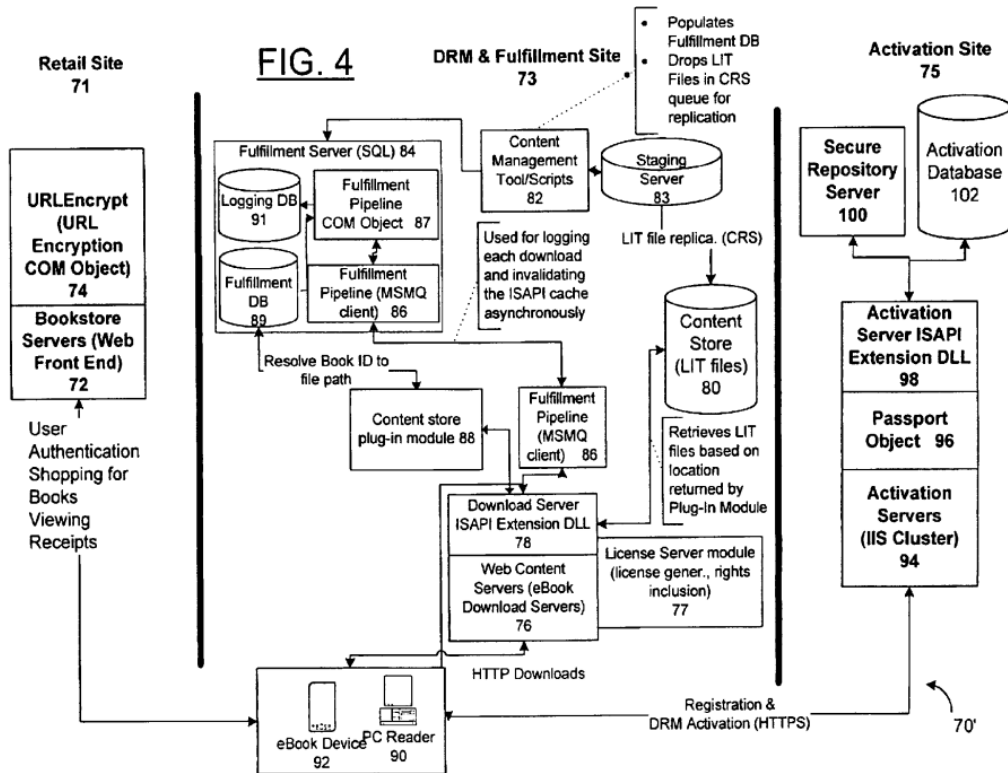
FIG. 1



DeMello, Figure 1

b. DeMello's Architecture

99. The DRM system of DeMello “define[s] an architecture for sharing information between a reader, a content provider and a content source, how that information is used to ‘seal’ titles at the various levels, and how that information must be structured.” (NF-1006, DeMello, 6:22-26.) DeMello discloses a server architecture, illustrated in Figure 4 below, “for a digital rights management system that distributes and protects rights in content.” (NF-1006, DeMello, Abstract.) The architecture provides the functions of “encryption of source eBooks, conversion to the target reader format, generation of the license construct defining the rights granted to the user (in level 5 titles), sealing of the content prior to download in accordance with requirements (e.g., a level of protection) set forth by the publication provider, and download of ebook titles.” (NF-1006, DeMello, 8:53-59.) The server architecture includes “a retail site which sells content items to consumers, a fulfillment site which provides to consumers the content items sold by the retail site, and an activation site which enables consumer reading devices to use content items having an enhanced level of copy protection.” (NF-1006, DeMello, Abstract.)



DeMello, Figure 4

100. In this architecture, bookstore servers 72 “host the commercial web site that allow users to perform actions such as shopping for eBook titles, establishing their membership relationship with the retailer, paying for their transactions, and/or accessing the proof of purchase pages (server-side receipts).” (NF-1006, DeMello, 11:1-6.) URL encryption object 73 “encrypts a set of parameters relating to an eBook 10 that has been purchased on bookstore server 72.” (NF-1006, DeMello, 9:17-19; 11:6-17.) URL encryption object 74 “may encrypt these parameters using a secret (e.g., a symmetric cryptographic key) shared between bookstore server 72 and web content server 76.” (NF-1006, DeMello, 9:20-22.) The encrypted

parameters “may include an identification of the eBook purchased, information about the purchase such as the purchaser's name or credit card number or a transaction ID (e.g., in the case of level 3 or 5 titles), and a timestamp.” (NF-1006, DeMello, 9:22-26.) As taught by DeMello, these “parameters listed above are exemplary, and different parameters could be used without departing from the spirit and scope of the invention.” (NF-1006, DeMello, 9:27-30.) The encrypted parameters are “included in an HTTP request that points to web content server 76, such that content server 76 can fulfill the purchase made at bookstore server 72.” (NF-1006, DeMello, 9:30-33.) The content server 76 “validate[s] the encrypted parameters, authenticate[s] the retailer via a shared secret (e.g., a symmetric key used to encrypt the parameters), avoid[s] playback attacks, and determine[s] the content to download to end-users.” (NF-1006, DeMello, 11:8-17.)

101. Content server 76 “fulfill[s] the purchase made at bookstore server 72.” (NF-1006, DeMello, 9:32-33.) IASPI DLL 78 “is responsible for validating download requests, retrieving the appropriate eBook file 10 from the content store 80 via content store plug-in module 88, individually sealing copies, returning the eBook titles 10 to end-users, and logging the transaction into the fulfillment database 84.” (NF-1006, DeMello, 10:3-8.) License server module 77 “is responsible for generating and sealing licenses for level 5 protected LIT files.” (NF-1006, DeMello, 11:44-47.) A license is “a construct that defines the rights that

the rights that the user may exercise upon purchase of an eBook title.” (NF-1006, DeMello, 11:47-49.) License server module 77 “validates the activation certificate of the user to whom the eBook is being downloaded and signs each license with the private key of the fulfillment center provider, which will later allow reader 90 or 92 to authenticate the distribution channel when the downloaded LIT file is accessed on such reader.” (NF-1006, DeMello, 11:49-55.)

102. Content store 80 “serves as a repository for LIT titles (eBooks 10) used by the download server ISAPI 78 when fulfilling orders for eBooks 10.” (NF-1006, DeMello, 10:25-28; 12:9-11.) “Content management and encryption tool 82 is a component that performs functions such as converting content to the LIT format (e.g., eBook 10), encrypting and sealing each eBook title on the content store 80.” (NF-1006, DeMello, 10:33-36.) Content management and encryption tool 82 “updates fulfillment database 84 with the physical location of each LIT file on the content store 80, which is mapped to their unique ID on the fulfillment database 84.” (NF-1006, DeMello, 10:36-40.) Content store plug-in module 88 “is responsible for determining the physical location on the content store 88 of each of the LIT files (eBooks) being downloaded, based on a combination of parameters (e.g., book ID and book ID type parameters) included on the download request (i.e., the encrypted parameters attached to the URL).” (NF-1006, DeMello, 11:33-39.)

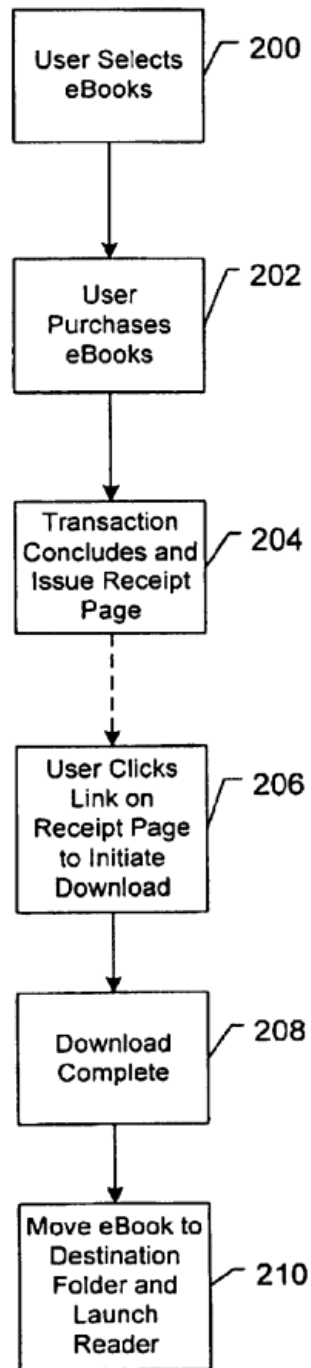
103. Fulfillment database 84 “hosts tables that map the combination of ‘Book ID’ and ‘Book ID Type’ to the physical location of each LIT file on content store 80.” (NF-1006, DeMello, 12:23-26.) Database 84 also “contains information about each LIT file that may be required for fulfillment, such as the book title, the book author, DRM protection level, and/or suggested retail price.” (NF-1006, DeMello, 12:25-28.)

104. Turning next to the activation site, “activation servers 94 perform the function of providing each client reader (e.g., PC reader 90 or dedicated reading device 92) with a unique secure repository and an activation certificate.” (NF-1006, DeMello, 13:14-17.) The secure repository and activation certificate associates an activated reader with an online persona “to ensure that users will be able [to] read their rightfully acquired titles on all instances of readers that they own or have activated to their persona.” (NF-1006, DeMello, 13:21-26.) Secure repository servers 100 “generat[e] individualized secure repositories for each reader being activated.” (NF-1006, DeMello, 14:8-11.) Activation database 102 “stores activation information related to each end-user of the reader 90 or 92” including “Machine IDs, the number of activated readers, the date of first activation, the product ID (PID) for each of the reader installations, their PASSPORT™ profile info, etc.” (NF-1006, DeMello, 14:24-30.) “This information is used to ensure that users are not abusing the system, helping users

recover from hard-drive crashes, and aiding in allowing users to continue reading the content they purchased after a hardware upgrade.” (NF-1006, DeMello, 14:31-33.)

c. eCommerce Process Flow

105. DeMello’s “process by which eBook titles are acquired and delivered online”, illustrated in Figure 9 below, begins in step 200 when a “user chooses book(s) via mechanism that the retail site implements.” (NF-1006, DeMello, 25:66-67, 26:2-3.) In step 204, when the transaction completes, the retail site generates “a receipt page (i.e., an order confirmation or ‘thank you’ page) that contains links (POST requests) for downloading each title purchased (i.e., the URLs containing the address of content server 76, plus the encrypted information created by URL encryption object 74).” (NF-1006, DeMello, 26:4-11.) For level 5 content, a client-side script executing at the user device “populate[s] the body of the POST with the activation certificate, preferably using COM object implemented by the reader which obtains the necessary activation certificate or relevant information therefrom.” (NF-1006, DeMello, 26:11-15.)

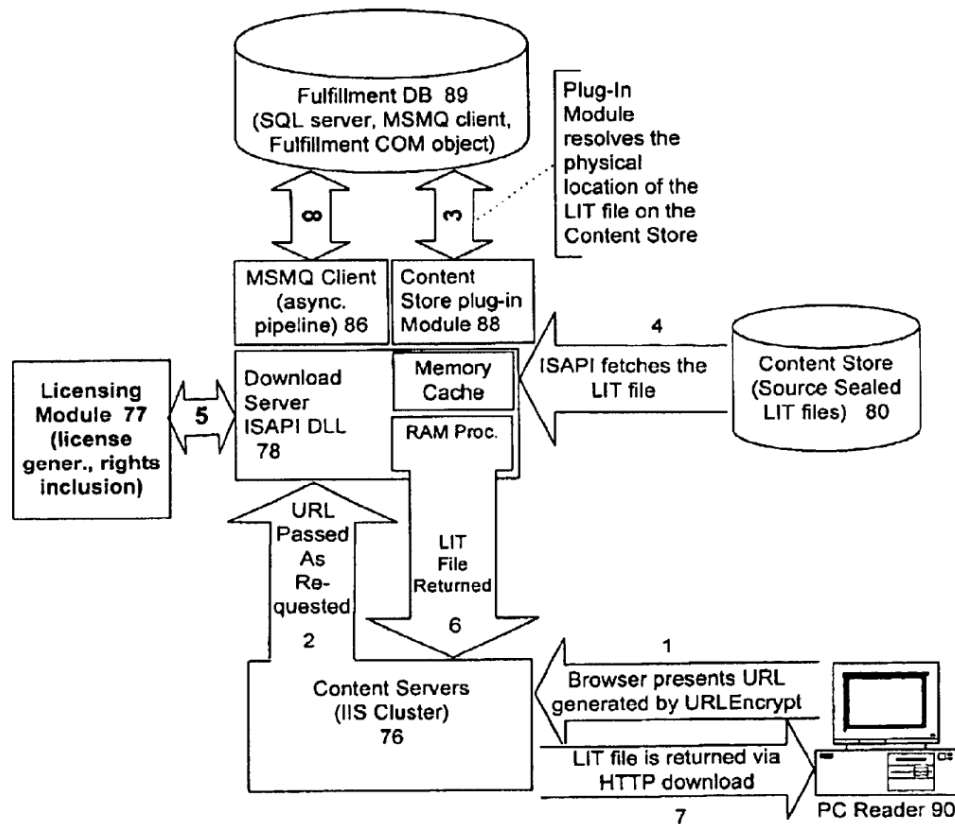


DeMello, Figure 9

106. When the user clicks on the links in the POST message, the browser at the user's device initiates a "download from content servers 76 (via the download

server ISAPI DLL 78).” (NF-1006, DeMello, 26:16-18.) For level 3 content, “the download server 76 adds the consumer's name to the title meta-data and re-seal the symmetric key 14A using a new cryptographic hash resulting from the new meta-data, which now includes the users name.” (NF-1006, DeMello, 26:18-23.) For level 5 content, “a license is generated and embedded in the LIT file, in addition to the Bookplate being created.” (NF-1006, DeMello, 26:23-25.) The license “contains the symmetric key 14A that encrypted the LIT file ‘sealed’ with the public key in the activation certificate.” (NF-1006, DeMello, 26:25-27.) “When the download is complete (step 208), the download server 76 logs the transaction and, on the client, the reader is launched automatically (step 210).” (NF-1006, DeMello, 26:27-30.)

107. DeMello describes the process of content fulfillment in further detail in Figure 10, reproduced below. In step 1, the client (user’s device) “makes a POST request to the download server” containing, at a minimum, “the encrypted blob generated by the URL encryption object.” (NF-1006, DeMello, 26:39-43.) This is equivalent to step 206 of Figure 9. For level 5 content, the request also “contain[s] the activation certificate” for the user’s device. (NF-1006, DeMello, 26:43-46.)



DeMello, Figure 10

108. The download server ISAPI 78 “extracts, from the body of the POST, the Retailer ID, which is required for fetching the symmetric key 75 associated with this retailer for decrypting the URL” (step 2). (NF-1006, DeMello, 26:47-50.) The server then “decrypts and validates the download request.” (NF-1006, DeMello, 26:50-51.) In step 3, the ISAPI 78 “passes the Book ID and Book ID type to the content store plug-in module, which then returns the physical location of the LIT file on the content store based on either a memory cache entry (if the LIT file being

requested had been previously downloaded) or a lookup on the fulfillment database 89.” (NF-1006, DeMello, 26:61-67.)

109. If the Book ID is not found on the local memory cache of the ISAPI 78, in step 4, “the LIT file is retrieved from the content store 80 and copied into the local memory cache of the ISAPI.” (NF-1006, DeMello, 27:1-4.) “When the ISAPI caches the LIT files locally, it strips the LIT files from their symmetric keys 14A and stores them on a separate cache bucket, indexed by their respective ID, which may increase security.” (NF-1006, DeMello, 27:4-7.)

110. The ISAPI then performs one of the following steps “in accordance with the DRM level required for the LIT file being downloaded” (step 5). (NF-1006, DeMello, 27:9-11.) If the request is for a level 1 file, or the LIT file is not source sealed in the content store 80, “the IASPI preferably returns an error, indicating that the proper error condition (invalid request or an invalid title in the content store, respectively).” (NF-1006, DeMello, 27:13-17.) For level 2 titles, “the ISAPI return the file to the end-user, with no processing done on the file whatsoever.” (NF-1006, DeMello, 27:18-29.) For level 3 titles, “the user's name will be inserted into a new stream in the LIT file, the meta-data stamped with level 3 (for use by the reader client 90 or 92), the new meta-data is hashed, and the symmetric key 14A used to encrypt the LIT file is sealed with the new cryptographic hash value computed.” (NF-1006, DeMello, 27:21-26.) For level 5 titles, “the ISAPI 78 will,

in addition to generating the functions note above for level 3, post a request to the licensing module 77, which will generate a license XrML blob, sign it with the fulfillment center's certificate, seal it with the end-user's activation public key, and return it for embedding in the LIT file.” (NF-1006, DeMello, 27:28-33.)

111. The ISAPI DLL “returns the LIT file to the IIS server 76 for download” (step 6) and the “LIT file is downloaded by IIS to the end-user via HTTP” (step 7). (NF-1006, DeMello, 27:40-50.) The ISAPI DLL then “use[s] the asynchronous fulfillment pipeline ... to log the transaction into the logging database 91 for later reporting and/or billing.” (NF-1006, DeMello, 27:51-61.)

112. After the eBook title has been downloaded to the client (after step 7), “the reader client may be launched.” (NF-1006, DeMello, 27:63-64.) “This is enabled via a file-extension association of LIT to the reader.” (NF-1006, DeMello, 27:64-65.)

2. Schwartz

113. Schwartz discloses a method “for facilitating the validation of content over a network.” (NF-1007, Schwartz, 4:62-64.) In Schwartz, a central content registration authority “registers the content disseminated by one or more content providers to one or more client devices.” (NF-1007, Schwartz, 5:44-46.) “A client device which receives registered content can securely consume the content, based on an assumption that the content provider that furnished the content is entrusted

by the content registration authority to provide the content, and without prompting a user of the client device to expressly approve the content provider.” (NF-1007, Schwartz, 5:46-52.) Validation “proceeds in a transparent manner with respect to the providers of content (from the perspective of the receiving client devices), resting solely on the authority associated with the central registration authority.” (NF-1007, Schwartz, 5:52-56.)

114. Schwartz describes two approaches for improving content security. According to a first solution (‘solution A’), “registration may comprise forming a content identifier based on the content (e.g., a hash of the content), and then, at the content registration authority, forming a stamp based on the content identifier.” (NF-1007, Schwartz, 5:57-61.) The “content publisher forwards the stamp along with the content to a client device. In this case, validation at the client device can comprise, in part, using the stamp to determine whether the integrity of the content is vouched for by the content registration authority.” (NF-1007, Schwartz, 5:61-65.)

115. According to the second solution (‘solution B’), “registration may comprise storing the content identifier in a registration store maintained by the content registration authority.” (NF-1007, Schwartz, 5:67-6:2.) “In this case, validation at the client device may comprise determining whether received content

has a corresponding registered content identifier stored at the content registration authority.” (NF-1007, Schwartz, 6:2-5.)

116. The implementation of Schwartz’s system for “solution B” is illustrated in Figure 5 below. In this solution, content registration authority 332 “receives a content identifier from the content publisher.” (NF-1007, Schwartz, 10:64-66.) The content publisher “forms the content identifier by computing a digest of the content 330, such as a hash of the content.” (NF-1007, Schwartz, 10:66-11:1.) Upon receipt of the content identifier, the content registration authority 332 “store[s] the content identifier in a registration data store, thereby effectively registering the content identifier.” (NF-1007, Schwartz, 11:1-4.)

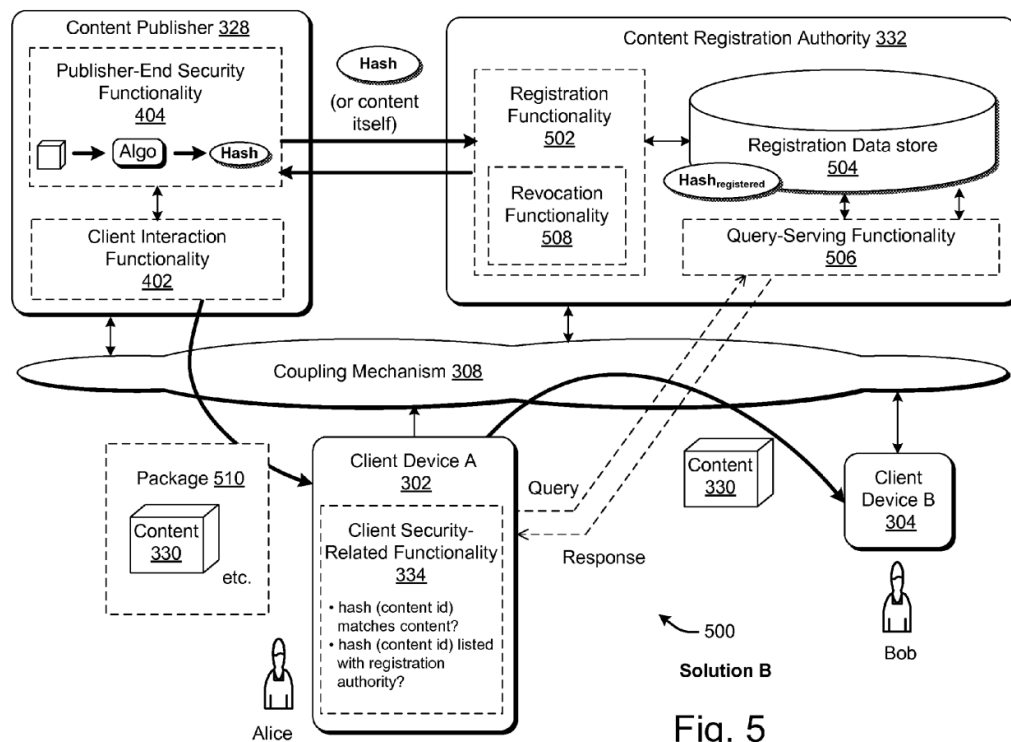


Fig. 5

Schwartz, Figure 5

117. The content publisher 328 then “transfer[s] the content 330 to the client device A.” (NF-1007, Schwartz, 11:4-6.) To verify the integrity of the content 330, the client device A 302 independently “compute[s] the content identifier of the received content 330, e.g., by forming a hash of the received content.” (NF-1007, Schwartz, 11:6-9.) The client device A 302 then “use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration authority 332.” (NF-1007, Schwartz, 11:9-12.) If this test passes, “the client device A 302 assesses that the content 330 is trustworthy, regardless of the specific identity of the content publisher 328 used to furnish the content 330.” (NF-1007, Schwartz, 11:12-16.)

118. A procedure corresponding to solution B is illustrated in Figure 9 below. As discussed above, “Solution B involves the registration of content items by storing them in the registration data store 504.” (NF-1007, Schwartz, 25:23-25.) In step 902, “publisher-end security functionality 404 computes a hash of the newly created content 330 sends it to the content registration authority 332.” (NF-1007, Schwartz, 25:30-32.) Alternatively, “publisher-end security functionality 404 can transfer the content 330 itself to the content registration authority 332, upon which the content registration authority 332 can use its own resources to process the content 330 and form the hash.” (NF-1007, Schwartz, 25:32-36.)

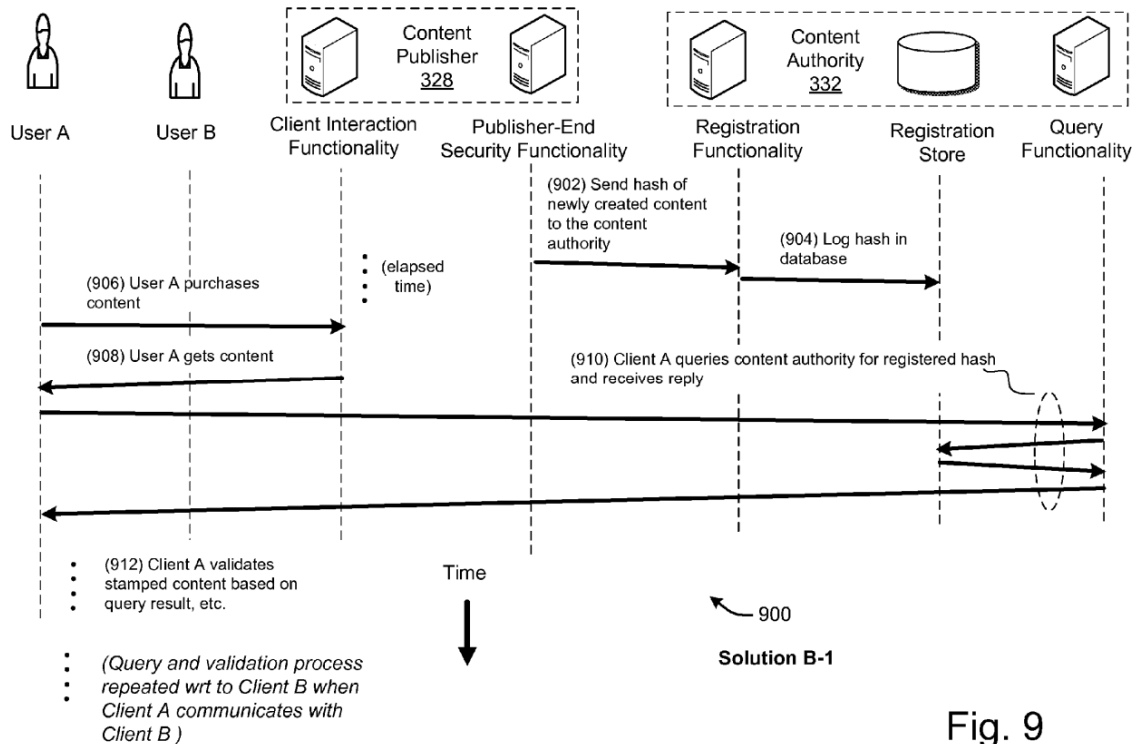


Fig. 9

Schwartz, Figure 9

119. In step 904, “registration functionality 502 receives the hash and stores it in the registration data store 504.” (NF-1007, Schwartz, 25:37-38.) Later, “in step 906, the user, Alice, can purchase the content 330 that has been registered in the registration data store 504.” (NF-1007, Schwartz, 25:39-41.) In step 908, the client interaction functionality 402 “download[s] the purchased content 330 to Alice's client device A 302.” (NF-1007, Schwartz, 25:44-46.) In steps 910 and 912, Alice's client device A 302 “validat[es] the received content.” (NF-1007, Schwartz, 25:47-48.) “Validation for solution B comprises contacting the query functionality 506 to determine whether there is a counterpart registered content identifier stored in the registration data store 504, and if so, returning a result of

this lookup to the client device A 302.” (NF-1007, Schwartz, 25:48-52.) Alice's client device A 302 “compute[s] a separately computed content identifier (based on the received content 330 itself) and use[s] this information as an index to determine whether the content has been previously registered in the data store 504.” (NF-1007, Schwartz, 25:52-57.)

3. Walmsley

120. Walmsley relates to validating untrusted objects and entities. (NF-1008, Walmsley, Title.) Walmsley describes the use of hash functions. Specifically, Walmsley explains that “[s]pecial one-way functions, known as Hash functions, map arbitrary length messages to fixed-length hash values.” (NF-1008, Walmsley, 9:54-55.) As discussed in Walmsley, the “primary application for hash functions is in the reduction of an input message into a digital ‘fingerprint’ before the application of a digital signature algorithm.” (NF-1008, Walmsley, 10:3-5.) However, a “one-way hash function is not sufficient protection for a message.” (NF-1008, Walmsley, 11:43-44.) For example, a “simple attack by E, who is in-between A and B, is to intercept the message from B, and substitute his own.” (NF-1008, Walmsley, 11:45-47.) “Even if A also sends a hash of the original message, E can simply substitute the hash of his new message.” (NF-1008, Walmsley, 11:47-49.)

121. Walmsley teaches that a solution to this problem “is the Message Authentication Code, or MAC.” (NF-1008, Walmsley, 11:52-53.) With a MAC, “[w]hen B sends message M, it also sends MAC[M] so that the receiver will know that M is actually from B.” (NF-1008, Walmsley, 11:55-56.) For this to be possible, “only B must be able to produce a MAC of M, and in addition, A should be able to verify M against MAC[M].” (NF-1008, Walmsley, 11:56-58.) “The simplest method of constructing a MAC from a hash function is to encrypt the hash value with a symmetric algorithm.” (NF-1008, Walmsley, 11:61-63.) “Any symmetric or asymmetric cryptographic function can be used.” (NF-1008, Walmsley, 11:67-12:1.)

122. Walmsley specifically discloses use of HMAC which was “gaining acceptance as a solution for Internet message authentication security protocols.” (NF-1008, Walmsley, 12:32-34.) An HMAC uses a “secret key shared by the two parties” to compute the hash. (NF-1008, Walmsley, 12:41-67.) As explained by Schneier, with an HMAC, only an individual with an identical key can verify the hash. (NF-1009, Schneier, 455.)

4. Motivation to Combine

123. A POSITA would have been motivated to use Schwartz’s solution B with DeMello’s DRM system. While DeMello discloses the transmission of a content file having content encrypted using an encrypted symmetric key, DeMello does not

provide a technique to authenticate that the received content is the actual content stored in the content database by the content provider. A POSITA would have therefore been motivated to add additional security to ensure the authenticity and integrity of the content retrieved by the end-user device and would have been led to Schwartz. As I discussed in the Technology Background, integrating security mechanisms to authenticate data and verify integrity of message contents were common and well-known by January 2014. (*See* §IV.A.) Like the '102 patent and DeMello, Schwartz discloses a digital rights management system. Specifically, Schwartz provides a technique to authenticate and validate the integrity of content as discussed in §IV.A.2. Schwartz is therefore in the same field as the '102 patent and is reasonably pertinent to the subject matter of the '102 patent.

124. In the combined system of DeMello and Schwartz, the content store of DeMello uses a hash of the content as the Content ID (e.g., Book ID). When the client device (e.g., DeMello's reader) receives content in the combined system, the client device calculates the hash of the content and shares that value with the content registration authority (DeMello's content source) which validates the existence of the hash in its database. If the hash exists, the client device confirms that the content provided by the content provider is the authentic because any alternation of the content results in a different hash value than the value stored in the content store. If the hash does not exist in the content store, the content has

been altered in some way and the client terminates processing and does not access the content. Thus, the combination of DeMello and Schwartz ensures that a client device (reader) uses only authentic content that has not been altered.

125. As I discussed in §VI.A.2, Schwartz discloses the use of a one-way hash function to calculate a content ID for content. Schwartz does not disclose any details regarding the hash function used with its technique. Hash functions were well-known long before the filing date of the '102 patent. Schneier, published in 1996, describes a variety of one-way hash functions that were in use. (NF-1009, Schneier, 429-460.) And, RFC 2104, published in February 1997, describes HMAC, “a mechanism for message authentication using cryptographic hash functions.” (NF-1014, RFC 2104, 1.) Additionally, in Schwartz, the Content ID (hash) is transmitted to the content registration authority of the content provider without any additional security for verification. Therefore, a POSITA would have been motivated to integrate additional security into the hash to protect against attacks during transmission which would alter the value of the hash. A POSITA would have therefore been motivated to use a hash derived from a cryptographic key such as the well-known HMAC to allow the receiving party to confirm the integrity of the hash and authenticate the hash came from the expected end-user device.

126. A POSITA would have therefore been motivated to search for documents that teach the implementation details of these well-known keyed hash functions and would have been led to Walmsley. Walmsley is in the same field as Schwartz and the '102 patent—protecting data. Further, both Walmsley and Schwartz disclose the use of hash functions to generate fingerprints of data and therefore are reasonably pertinent to the disclosure of the '102 patent which discusses the generation of a fingerprint for content.

127. As I discussed in §VI.A.3, Walmsley discloses the use of Message Authentication Codes (MACs) and specifically the use of HMAC. A POSITA would have been motivated to use the MAC technique disclosed in Walmsley to compute the Content ID (e.g., Book ID) in the combined system of DeMello and Schwartz to provide enhanced security of the hash value. Specifically, the keyed hash ensures that the hash cannot be substituted for a different hash in transit. Walmsley motivates the combination explaining that a basic one-way hash function “is not sufficient protection for a message.” (NF-1008, Walmsley, 11:42-43.) Specifically, Walmsley explains that one-way hash functions are susceptible to man-in-the-middle attacks where an attacker, E, between A and B, intercepts a message and substitutes his own message. (NF-1008, Walmsley, 11:45-47.) A POSITA would understand that because Schwartz transmits messages between the end-user device and content providing server, Schwartz’s hash is susceptible to the

man-in-the middle attack where a malicious party alters the transmitted hash. For example, a malicious individual could alter content stored in the network database and simply replace the stored content ID with a content ID for the modified content. This attack opens the content database up to injection of viruses or other malware. A POSITA would have therefore been motivated to use Walmsley's MAC as the Content ID in Schwartz to provide integrity of the content ID when stored in the network (from Content Provider to Content Host) and when transmitted to the content provider for verification.

B. Independent Claim 10

128. The combination of DeMello, Schwartz, and Walmsley renders claim 10 obvious. For ease of discussion, I have reproduced the text of independent claim 10 again.

[10P] *A method, comprising:*

[10A] *obtaining an access restricted content from at least one of a content database and a content providing server;*

[10B] *obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the query comprising the content identifier and an identifier associated with the user;*

[10C] *deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based at least in part on the first digital rights management key,*

[10D] *causing the content providing server to validate the fingerprint, and, if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and*

[10E] *deriving, using the digital rights management header of the access restricted content, from the access restricted content a second and third digital rights management key,*

[10F] *wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and*

[10G] *wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key,*

[10H] *wherein the content is usable without being in an unprotected state*

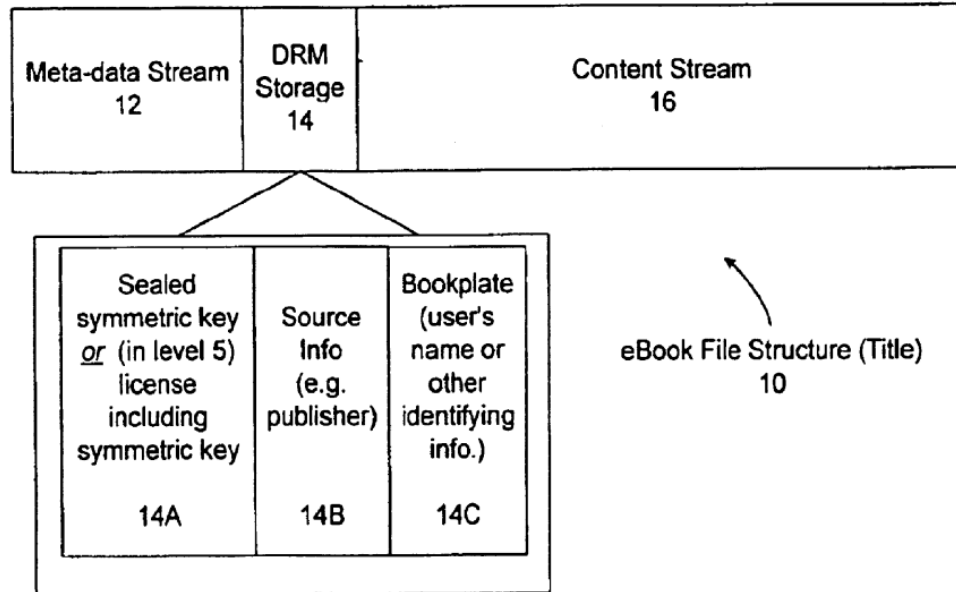
1. Preamble [10P]

129. DeMello is directed to a system and method “for processing and delivery of electronic content wherein the content may be protected at multiple levels.” (NF-1006, DeMello, 4:41-43.) The preferred embodiment described in DeMello “is directed to the processing and delivery of electronic books, however, the invention is not limited to electronic books and may include all digital content such as video, audio, software executables, data, etc.” (NF-1006, DeMello, 4:44-49.) DeMello therefore discloses a “*method*” [10P].

2. “Obtaining an access restricted content” [10A].

130. DeMello’s content file, illustrated in Figure 1 below, “contains content 16, which is text such as a book (or any electronic content) that has been encrypted by a key (the ‘content key’), which itself has been encrypted and/or sealed.” (NF-1006, DeMello, 6:38-42.) The encrypted content 16 is therefore “*access restricted content.*”

FIG. 1



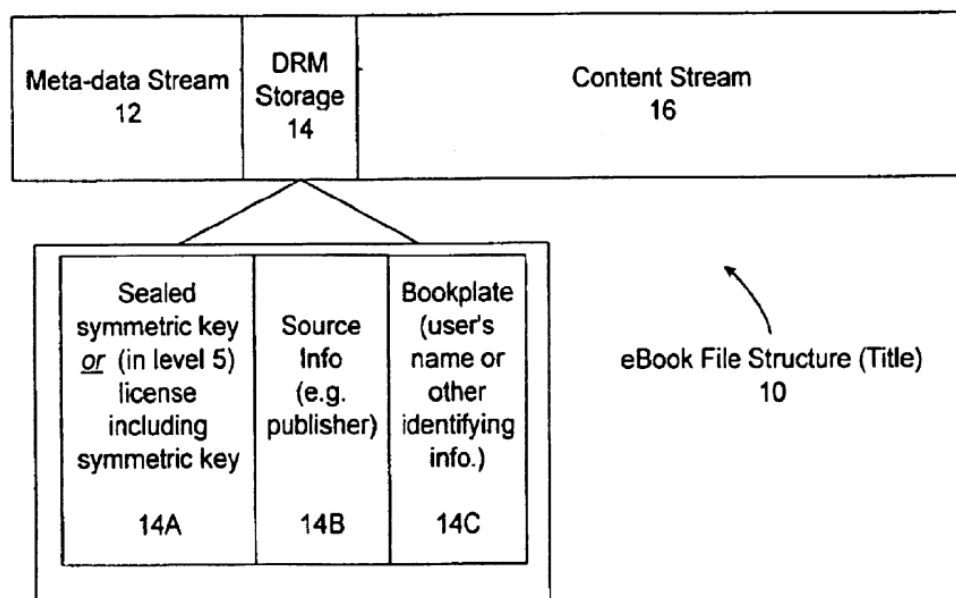
DeMello, Figure 1

131. In §VI.A.1, I described DeMello’s server architecture. In operation, a user selects content (e.g., a book) via a mechanism implemented by a retail site selling content. (See NF-1006, DeMello, 26:2-3.) When the purchase transaction completes, the retail site generates “a receipt page (i.e., an order confirmation or

‘thank you’ page) that contains links (POST requests) for downloading each title purchased (i.e., the URLs containing the address of content server 76, plus the encrypted information created by URL encryption object 74).” (NF-1006, DeMello, 26:4-11.) For level 5 content, a client-side script executing at the user device “populate[s] the body of the POST with the activation certificate, preferably using COM object implemented by the reader which obtains the necessary activation certificate or relevant information therefrom.” (NF-1006, DeMello, 26:11-15.)

132. When the user clicks on the link provided in the POST message from the retail site, the browser at the user’s device initiates a “download from content servers 76 (via the download server ISAPI DLL 78).” (NF-1006, DeMello, 26:16-18.) Content server 76 at the Fulfillment Site is “*a content providing server.*” For level 5 content, a license is generated at the Fulfillment Site “and embedded in the LIT file, in addition to the Bookplate being created.” (NF-1006, DeMello, 26:23-25.) The LIT file is illustrated in Figure 1 below. The license “contains the symmetric key 14A that encrypted the LIT file ‘sealed’ with the public key in the activation certificate.” (NF-1006, DeMello, 26:25-27.)

FIG. 1

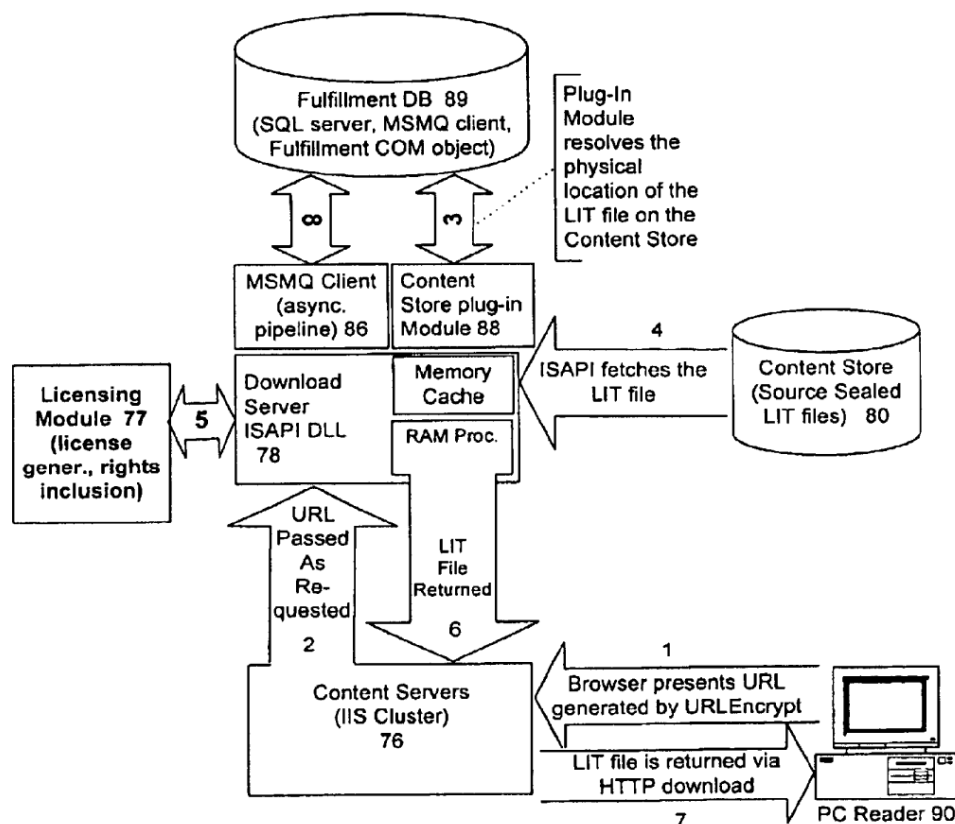


DeMello, Figure 1

133. DeMello describes the process of content download to the user device in Figure 10, reproduced below. Upon receipt of the POST request, the download server ISAPI 78 at the Fulfillment Site “extracts, from the body of the POST, the Retailer ID, which is required for fetching the symmetric key 75 associated with this retailer for decrypting the URL” (step 2). (NF-1006, DeMello, 26:47-50.) The server then “decrypts and validates the download request.” (NF-1006, DeMello, 26:50-51.) In step 3, the ISAPI 78 “passes the Book ID and Book ID type to the content store plug-in module, which then returns the physical location of the LIT file on the content store based on either a memory cache entry (if the LIT file being

requested had been previously downloaded) or a lookup on the fulfillment database 89.” (NF-1006, DeMello, 26:61-67.)

134. The ISAPI then performs one of the following steps “in accordance with the DRM level required for the LIT file being downloaded” (step 5). (NF-1006, DeMello, 27:9-11.) For level 5 titles, “the ISAPI 78 will, in addition to generating the functions note [sic] above for level 3, post a request to the licensing module 77, which will generate a license XrML blob, sign it with the fulfillment center's certificate, seal it with the end-user's activation public key, and return it for embedding in the LIT file.” (NF-1006, DeMello, 27:28-33.) The ISAPI DLL “returns the LIT file to the IIS server 76 for download” (step 6) and the “LIT file is downloaded by IIS to the end-user via HTTP” (step 7). (NF-1006, DeMello, 27:39-50.) Thus, the end-user device obtains the content from the content providing server at the Fulfillment Site.



DeMello, Figure 10

135. DeMello therefore discloses “*obtaining an access restricted content from at least one of a content database and a content providing server.*”

3. “*Fingerprint*” Limitations

136. Independent claim 10 recites the following three limitations directed to the “*fingerprint of the access restricted content.*” As I detail in this section, the combination of DeMello, Schwartz, and Walmsley teaches these limitations.

[10B] *obtaining a first digital rights management key from a content database, wherein the obtaining is based at least in part on a query, the*

query comprising the content identifier and an identifier associated with the user;

[10C] *deriving, using the first digital rights management key, from the access restricted content a fingerprint of the access restricted content wherein the obtaining is based³ at least in part on the first digital rights management key;*

[10D] *causing the content providing server to validate the fingerprint*

137. In Schwartz's Solution B, illustrated in Figure 9 below, the hash of the content is stored in a registration data store 504 (step 904). (NF-1007, Schwartz, 25:37-38.) After content is downloaded to the client device, client device A 302 "validat[es] the received content." (NF-1007, Schwartz, 25:47-48.) "Validation for solution B comprises contacting the query functionality 506 to determine whether there is a counterpart registered content identifier stored in the registration data store 504, and if so, returning a result of this lookup to the client device A 302." (NF-1007, Schwartz, 25:48-52.) The client device "compute[s] a

³ Claim 10 lacks a clear antecedent basis for the phrase "*the obtaining is based at least in part on the first digital rights management key.*" The phrase could apply to either the "*obtaining an access restricted content*" of limitation [10A] or the "*deriving*" of limitation [10C]. Solely for purposes of this IPR, I have been instructed to assume that "*obtaining is based ...*" applies to the "*deriving*" of limitation [10C] based on the parallel language of claim 1.

separately computed content identifier (based on the received content 330 itself) and use[s] this information as an index to determine whether the content has been previously registered in the data store 504.” (NF-1007, Schwartz, 25:52-57.)

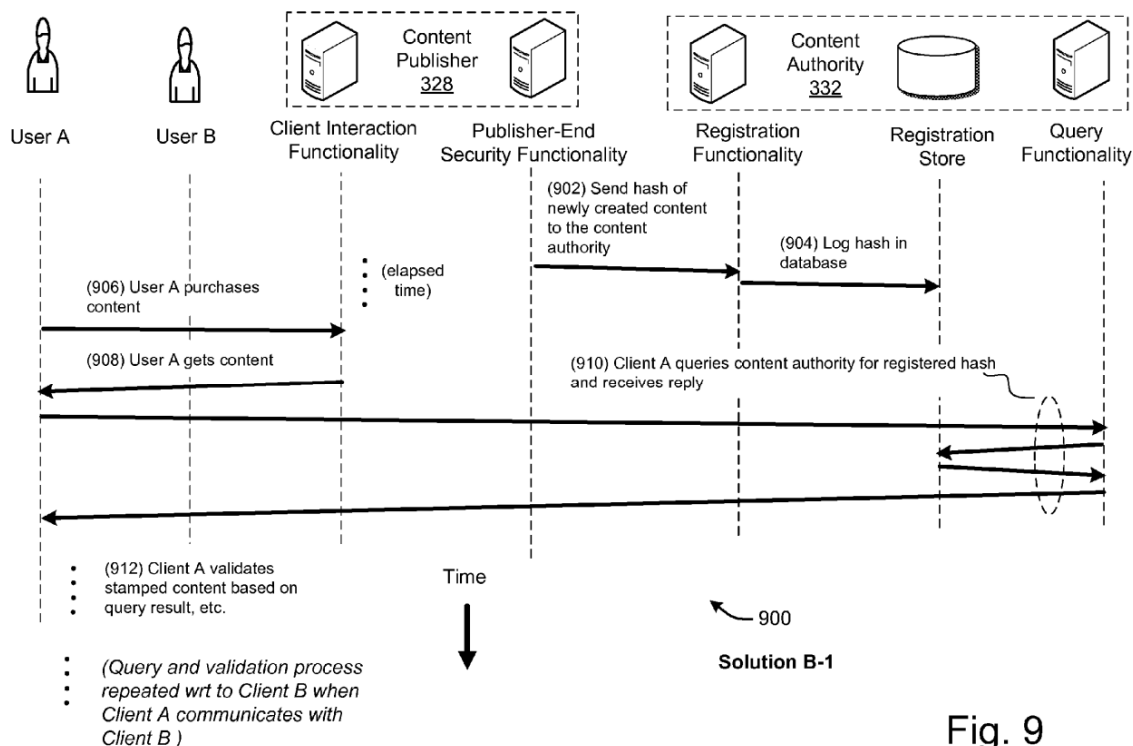


Fig. 9

Schwartz, Figure 9

138. In the proposed combination discussed in §VI.A.4, a POSITA would have been motivated to use a keyed hash for computing the Content ID (e.g., Book ID) in the combination of DeMello and Schwartz, as disclosed by Walmsley. Specifically, a POSITA would have been motivated to use Walmsley’s message authentication code which is a “key-dependent one-way hash function.” (NF-1009, Schneier, 455.) According to Walmsley, “the simplest method of constructing a MAC from a hash function is to encrypt the hash value with a symmetric

algorithm.” (NF-1008, Walmsley, 11:61-63.) Walmsley further describes a known MAC algorithm HMAC, which uses a hash function and a shared secret key. (NF-1008, Walmsley, 12:41-67.) The shared secret hash key is the “*first digital rights management key*.”

139. Walmsley discloses the use of a shared key for computing the MAC. Walmsley does not disclose that the symmetric hash key is shared by the content provider. However, a POSITA would have understood that in the combined system the shared symmetric hash key for the content would have been included in the content file with the shared encryption key (content key) for the content because it is a cryptographic key used to process the content stored in the content store (database) of DeMello. Like the content key, the shared hash key would have been sealed with the public key of the user’s activation certificate. Thus, the client device “*obtain[s] a first digital rights management key from a content database*” [10B] in the content file received by the user device.

140. In the combination of DeMello, Schwartz, and Walmsley, the client device “*compute[s] a separately computed content identifier based on the received content 330*” as taught by Schwartz using the key-dependent one-way hash function, the HMAC, disclosed by Walmsley. (See NF-1007, 21:25-28.) T The resulting key-hash value is a bit string and is unique representation of the content derived directly from the content—the recited “*fingerprint*.” Thus, the combination

of DeMello, Schwartz, and Walmsley discloses “*deriving, using the first digital rights management key [shared secret HMAC key], from the access restricted content a fingerprint of the access restricted content [the content identifier (keyed hash)] wherein the obtaining [deriving] is based at least in part on the first digital rights management key [shared secret HMAC key]*” [10C].

141. The client device “use[s] the computed content identifier as a key to determine whether the content has been previously registered in the registration data store of the content registration.” (NF-1007, Schwartz, 11:9-12.) That is, the user device transmits the keyed hash (“*fingerprint*”) to the content registration database at the Fulfillment Site which is DeMello’s content storage database (“*content database*”) in the combined system. The content database at the Fulfillment Site (“*content providing server*”) in the combined system validates the keyed hash by determining whether the keyed hash exists in the registration database of Content IDs. If the keyed hash exists, the content received at the client device is authentic and has not been altered. Thus, the combination teaches “*causing the content providing server to validate the fingerprint*” [10D].

4. “*Access[ing] Restricted Content*”

142. Independent claim 10 recites the following limitations directed to the “*accessing the access restricted content.*” As I detail in this section, the combination of DeMello, Schwartz, and Walmsley teaches these limitations.

[10D] ... if the validation is successful, accessing the access restricted content and information describing encryption properties of the access restricted content, and

[10E] deriving, using the digital rights management header⁴ of the access restricted content, from the access restricted content a second and third digital rights management key,

[10F] wherein the second and third digital rights management keys are applied to retrieve the payload of the access restricted content and

[10G] wherein at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key

143. In the combined system, if the content is determined to be authentic by the end-user device (i.e., the hashed content ID matches a content ID stored at the Fulfillment Site), the reader client is launched. (NF-1006, DeMello, 27:63-64.)

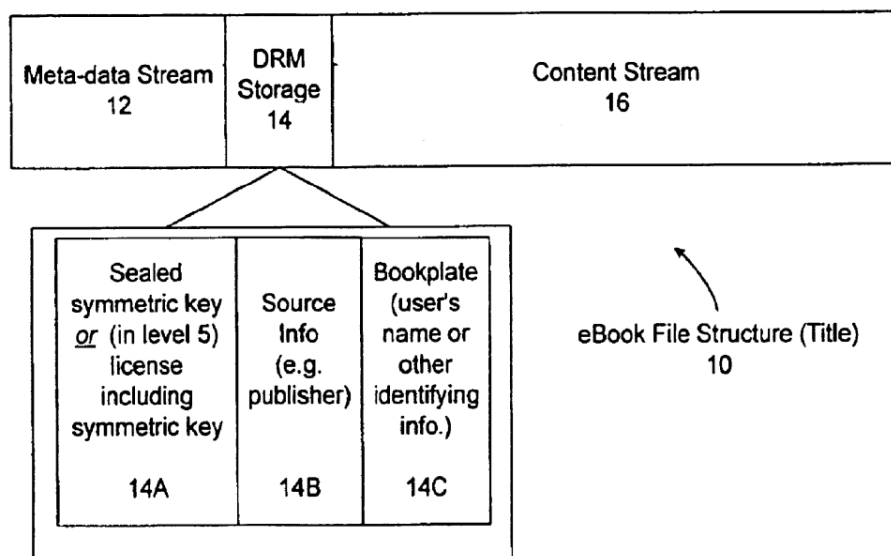
“‘Fully individualized’ titles can only be opened by authenticated reader applications that are ‘activated’ for a particular user, thereby protecting against porting of a title from one person’s reader (or readers) to a reader that is not registered to that person.” (NF-1006, DeMello, 6:11-16.) Thus, if the validation of

⁴ Claim 10 lacks antecedent basis for “the digital rights management header.” Solely for purposes of this IPR, Petitioner assumes the claim is intended to recite “a digital rights management header.” Petitioner reserves the right to argue indefiniteness of this term in another forum.

the authenticity of the content is successful, the reader application accesses the content file. DeMello therefore discloses “*if the validation is successful, accessing the access restricted content*” [10D].

144. In DeMello, a content file (e.g., eBook 10), illustrated in Figure 1 below, contains content 16 “that has been encrypted by a key (the ‘content key’), which itself has been encrypted and/or sealed.” (NF-1006, DeMello, 6:39-42.) The content key of DeMello is a “*second digital rights management key*.” As shown in Figure 1 below, the content key (encryption key) is stored in the license 14A for level 5 content. (See NF-1006, DeMello, 2:65; 6:48-53; 33:11-25.) The DRM storage 14 portion of the content file 10 is a “*digital rights management header*.” And for level 5 content, the content key is sealed “with the public key of the user’s activation certificate.” (NF-1006, DeMello, 6:45-48.) The public key of the user’s activation certificate and its associated private key (the asymmetric key pair for the activation certificate) are a “*third digital rights management key*.”

FIG. 1



DeMello, Figure 1

145. The end-user device further includes additional “code and data [that] are necessary to access ‘fully individualized’ content on a given client device.” (NF-1006, DeMello, 2:31–35.) The “‘data’ includes an activation certificate having a public key and an encrypted private key, and the ‘code’ is a program (e.g., a ‘secure repository’) that accesses the private key in the activation certificate by applying, in a secure manner, the key necessary to decrypt the encrypted private key.” (NF-1006, DeMello, 2:35-40; *see also* 24:14–17 (“the activation certificate for a given device contains its private key in a form encrypted by the public key associated with the secure repository”).) The secure repository on the user’s device “hides cryptographic keys used in the process of unsealing and decrypting level 5 LIT files.” (NF-1006, DeMello, 25:9-11.) This additional code and data is

“information describing encryption properties of the access restricted content” and DeMello therefore teaches *“if the validation is successful, accessing ... information describing encryption properties of the access restricted content”* [10D].

146. For level 5 content, the secure repository uses its private key to decrypt the private key of the activation certificate (*“third digital rights management key”*), which, in turn, is then used to decrypt the symmetric key 14A (*“second digital rights management key”*) of the eBook title, which, in turn, **is used to decrypt the content stream 16 of the eBook title.**” (NF-1006, DeMello, 24:19–23, 6:36–7:2 (“Referring to FIG. 1, eBook 10 contains content 16, which is text such as a book (or any electronic content) that has been encrypted by a key (the ‘content key’), which itself has been encrypted and/or sealed. In a preferred embodiment, the key is a symmetric key 14A that is sealed ... with the public key of the user’s activation certificate. ... In the case of level 5 titles, instead of storing the content key as a separate stream, stream 14A contains a license, which is a construct that defines the rights that the user can exercise upon purchase of the title. In titles that have a license, the content key is contained within the license.”).) Thus, the second digital rights management key (the symmetric key for the content) is encrypted using the third encryption key (the public key portion of the asymmetric key pair for the activation certificate). Accordingly, DeMello discloses *“deriving, using the digital rights management header of the access restricted content, from the access*

restricted content a second and third digital rights management key” [10E], “the second and third digital rights management keys are applied to retrieve the payload of the access restricted content” [10F], and “at least one of the second or third digital rights management key is used to encrypt the other key of the second or third digital rights management key” [10G].

147. Claim 10 further recites that the “*content is useable without being in an unprotected state*” [10H]. The specification includes a single mention of the state of content. Specifically, the specification indicates “the client is able to use the content without leaving it in an unprotected state” in the third method described in the specification. (See §IV.B.) In this method, the content is maintained in the network and not stored in any format on the client device. Content not “*in an unprotected state*” is protected content. Therefore, as written, this limitation recites the content is usable when the content is in a protected state (e.g., encrypted). A POSITA would have understood that encrypted (protected) content is not directly useable by the client device. The client device must first decrypt the content. Should Patent Owner contend this limitation covers the circumstance where content is stored in encrypted form and then decrypted using a stored decryption key, such a process is (1) not disclosed in the ’102 patent and (2) was extremely well-known for decades prior to the ’102 patent as discussed in both Subramanya and Rosenblatt.

148. As I discussed above, DeMello's content file includes content encrypted using the symmetric key provided in the license portion of the content file. DeMello teaches that the reader "move[s] the file into the local library folder (e.g., 'C:\MyLibrary')." (NF-1006, DeMello, 27:66-67.) Each time the reader device displays the content (e.g., the eBook), the reader must decrypt the content using the symmetric key provided in the license. Therefore, in DeMello, content is stored in the client device in encrypted form and decrypted in real-time when the content is consumed by the user.

C. Dependent Claim 11

149. The combination of DeMello, Schwartz, and Walmsley renders dependent claim 11, reproduced below, obvious.

11. The method of claim 10, wherein the first digital rights management key is unique to a specific session.

150. The '102 patent provides limited discussion of the use of a session key, mentioning only once in the detailed description that "[a]t least one of the first, second and third digital rights management keys may be, depending on the embodiment, arranged to be session-specific in the sense that it is generated dynamically for use in a single session." (NF-1001, '102 patent, 8:61-67.) The '102 patent provides no detail on how a session key is generated for any of its

embodiments or for any of the first, second, or third digital rights management keys.

151. The use of session keys in secure protocols was well-known and in wide use for decades prior to the '102 patent. For example, Schneier, in “Applied Cryptography,” published in 1996 describes that “[i]n most practical implementations public-key cryptography is used to secure and distribute **session keys.**” (NF-1009, Schneier, 33.) As explained by Schneier, “Bob sends Alice his public key”, “Alice generates a random session key” and “encrypts it using Bob’s public key and sends it to Bob”, “Bob decrypts Alice’s message using his private key to recover the session key”, and both “encrypt their communications using the same session key.” (NF-1009, Schneier, 33.)

152. Walmsley also discloses the use of a session key. Walmsley explains that “a public key mechanism is used to transmit a symmetric session key, and then the session key is used for the actual messages.” (NF-1008, Walmsley, 5:57-59.) Thus, Walmsley teaches or at a minimum suggests the “*first digital rights management key is unique to a specific session.*”

VII. Conclusion

153. 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.

154. 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 this 2nd day of January 2023.

A handwritten signature in black ink, appearing to read 'Paul D. Martin', with a stylized, cursive script.

Dr. Paul D. Martin