Paper No. 1

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner,

v.

CONTENTGUARD HOLDINGS, LLC
Patent Owner.

Patent No. 7,523,072
Issued: April 21, 2009
Filed: December 16, 2005
Inventors: Mark J. Stefik, Peter L. T. Pirolli
Title: System For Controlling The Distribution And Use Of Digital Works

---

Inter Partes Review No. IPR2015-00445

Petition for *Inter Partes* Review of
U.S. Patent No. 7,523,072

Table of Contents

I. Introduction

A. Certification the ’072 Patent May Be Contested by Petitioner

Petitioner certifies that U.S. Patent No. 7,523,072 (Ex. 103) (the ’072 patent) is available for *inter partes* review. Petitioner also certifies it is not barred or estopped from requesting *inter partes* review of the claims of the ’072 patent. Neither Petitioner, nor any party in privity with Petitioner, has filed a civil action challenging the validity of any claim of the ’072 patent. The ’072 patent has not been the subject of a prior *inter partes* review by Petitioner or a privy of Petitioner. Petitioner also certifies this petition for *inter partes* review is timely filed as it is filed within one year of December 23, 2013, which is the date the Court in the Eastern District of Texas issued a summons on the basis of Patent Owner’s complaint for patent infringement of the ’072 patent against Apple in civil action No. 2:2013-cv-01112. *See* Ex. 1068. Because the date of this petition is less than one year from December 23, 2013, this petition complies with 35 U.S.C. § 315(b).

B. Fee for Inter Partes Review (§ 42.15(a))

The Director is authorized to charge the fee specified by 37 CFR § 42.15(a) to Deposit Account No. 50-1597.

C. Mandatory Notices (37 CFR § 42.8(b))

1. Real Party in Interest (§ 42.8(b)(1))

The real party of interest of this petition pursuant to § 42.8(b)(1) is Apple Inc. (“Apple”) located at One Infinite Loop, Cupertino, CA 95014.

2. Other Proceedings (§ 42.8(b)(2))

The ’072 patent is at issue in Civ. No. 2:2013-cv-01112 (E.D. Tx.), 2:14-cv-00061 (E.D. Tx.) and 3:14-cv-00498 (N.D. Cal.). IPR2015-00443 and -00444 filed concurrently also involve the ’072 patent. Each petition advances unique grounds based different primary references (*i.e.*, Kahn (Ex. 1018) and ABYSS (Ex. 1016)). The Kahn petition presents grounds based on the obvious combination of its server-based secure content distribution scheme with software-based client systems taught by Linn (Ex. 1058). The ABYSS petition presents grounds based on the obvious adaptation of its flexible copy protection system to use public-key encryption, alone or as implemented using the usage rights language technique of Hartrick (Ex. 1021). The present petition advances grounds based on the obvious adaptation of its hardware-based client and server DRM systems to use Hartrick’s usage rights language technique. Each petition presents a unique correlation of the claims to the prior art, and warrants independent institution of trial. In addition, Petitioner is challenging four other patents related to the ’072 patent, and has streamlined its challenges by asserting the same three prior art combinations against all of the patents. Petitioner respectfully requests the Board institute each petition, as each presents distinct and non-redundant grounds.

3. Lead and Backup Lead Counsel (§ 42.8(b)(3))

Lead Counsel	Backup Lead Counsel

Jeffrey P. Kushan (Reg. No. 43,401) jkushan@sidley.com (202) 736-8914	Michael R. Franzinger (46,335) mfranzinger@sidley.com (202) 736-8583

4. Service Information (§ 42.8(b)(4))

Service on Petitioner may be made by e-mail (iprnotices@sidley.com), or by mail or hand delivery to: Sidley Austin LLP, 1501 K Street, N.W., Washington, D.C. 20005. The fax number for lead and backup lead counsel is (202) 736-8711.

5. Proof of Service (§§ 42.6(e) and 42.105(a))

Proof of service of this petition is provided in **Attachment A**.

II. Identification of Claims Being Challenged (§ 42.104(b))

Claims **1, 8, 10, 16, 18, and 24** of the '072 patent ("the challenged claims") are unpatentable under 35 U.S.C. § 103 based on Patent No. 5,557,518 to Rosen ("Rosen") (Ex. 1020) in view of EP0567 800 to Hartrick ("Hartrick") (Ex. 1021). The evidence relied upon in support of this petition is listed in **Attachment B**.

III. Relevant Information Concerning the '072 Patent

A. Effective Filing Date

The '072 patent issued from U.S. Appl. No. 11/304,794, filed on December 16, 2005. Through continuation and divisional applications, the '794 application claims the benefit back to U.S. Appl. No. 08/344,760, filed on November 23, 1994. Solely for the purpose of this proceeding, Petitioner is treating the effective filing date of the '072 patent as not earlier than **November 23, 1994**.

B. Overview of the ’072 Patent

1. The ’072 Specification

The ’072 patent is a member of a family of patents issued to Stefik et al., including, *inter alia*, U.S. Patent Nos. 6,963,859; 7,269,576; 7,225,160; 8,370,956; and 8,393,007 (also subject to IPRs filed by Petitioner). Although designated “continuation” applications, the Stefik patents have non-identical disclosures, with varying degrees of overlap. Ex. 1013 at ¶ B2-B3.

The ’072 patent describes a scheme that allows authors to control the use and distribution of digital “content” (*e.g.*, software, books, video). Ex. 1003 at 6:38-7:2, Fig. 1. In this scheme, each copy of the content is encapsulated into a “digital work”—*i.e.*, a digital file to which “usage rights” are permanently attached and which is stored in and distributed via “repositories.” *See id.* at 6:16-17 (“A key feature of the present invention is that usage rights are permanently ‘attached’ to the digital work.”), 6:38-7:2, 50:34-36, 50:59-63. The “usage rights” data permanently attached to each copy of a digital work is used by repositories to control the manner in which a digital work can be used or distributed, as well as to specify any conditions on exercising those manners of use. *Id.* at 6:9-14, 6:16-17, 51:64-67. “Repositories” are “trusted devices” that store individual copies of digital works and regulate any copying or distribution of those copies by enforcing the usage rights attached to each work. *Id.* at 6:56-62, 6:22-26.

The ’072 patent explains digital works with “attached usage rights” and “repositories” are the two central features that provides its systems with “distinct advantages over prior systems.” *Id.* at 6:28-37, 6:35-44, 6:24-25, 6:16-17. Indeed, the ’072 patent shows that its scheme requires these two features to ***always*** be present – if either is removed, the author loses “control” of the work and the “content genie” can get “out of the bottle”:

> [I]n the prior art, payment of fees are primarily for the initial access. In such approaches, ***once a work has been read, computational control over that copy is gone***. Metaphorically, “***the content genie is out of the bottle*** and no more fees can be billed.” In contrast, ***the present invention never separates the fee descriptions from the work. Thus, the digital work genie only moves from one trusted bottle (repository) to another***, and all uses of copies are potentially controlled and billable.

Id. at 6:27-36, 6:18-21 (“the usage rights . . . assigned by a creator and subsequent distributor ***will always remain with a digital work***”), 6:22-23 (“The enforcement elements of the present invention are embodied in repositories.”). Thus, if content is separated from its usage rights or if a digital work is transferred to an untrusted system (*i.e.*, a system that is not a repository), nothing prevents a user from gaining unregulated access to the content, making unlimited copies of it or distributing unprotected content to others. *Id.*; Ex. 1013 at ¶ B11. In short, the scheme fails.

The ’072 patent indicates that authors can use these two “key elements” to

create different types of distribution schemes (*e.g.*, consumer redistribution, "commercial libraries," or paid distribution chains) by specifying particular manners of using and distributing each work, and setting conditions on such manners of use, in the usage rights attached to the digital work. Ex. 1003 at 43:19, 43:38, 43:62, 44:37, 44:59; 46:6. The '072 patent asserts being able to attach usage rights to digital works and to permit redistribution of content but only via repositories distinguishes its scheme over the prior art, particularly simple schemes which provide encrypted content then regulate the delivery and use of decryption keys to access that content. *Id.* at 2:3-5, 2:65-3:4, 3:45-50, 3:63-4:3. Contrary to the '072 patent's contentions, use of trusted systems and usage rights to regulate the distribution and use of digital content, including after delivery to a user, was well known before 1994. Ex. 1013 at ¶ A62-90, A91-97, B13-15; *see* Ex. 1016 at 38; Ex. 1027 at 1137; Ex. 1026 at 4; Ex. 1029 at 3:22-25; Ex. 1019 at Fig. 2.

2. Representative Claims

Independent claims 1, 10, and 18 each define a method for "*securely rendering digital documents*." *See* Ex. 1013 at ¶ C182. Claim 18 is representative, defining a 7-step method for transferring a "*digital document*" from a "*document repository*" to a "*document platform*": the document repository (i) receives "*a request . . . to transfer a digital document*," (ii) "*authenticat[es] the document platform*" and determines if it is "*authorized to use the digital document*," (iii)

"*determin[es] whether the [it]may be transferred and stored on the document platform based on a manner of use included in [] at least one usage right*", and (iv) "*transfer[s] the digital document and the at least one usage right[] to the document platform*." The document platform (v) stores the digital document "*in a separate file*" from the usage right(s), (vi) "*determin[es] . . . whether [it] may be rendered based on the at least one usage right*," and (vii) renders it.

Independent claims 1 and 10 specify a subset of the steps of claim 18, and claim 10 adds the step of having the document repository store the digital document and usage right in *separate files*. Dependent claims 8, 16, and 24 each specify that "*at least one part of the digital document and the at least one usage right are stored on a same device*."

C. The Person of Ordinary Skill in the Art

A person of ordinary skill in the relevant art in November 1994 would have been a person with a Bachelor of Science degree in Electrical Engineering, Computer Engineering, or Computer Science and either a Master of Science in one of those fields or two or more years of industry experience with designing and/or building cryptographic hardware or software. Ex. 1013 at ¶ A61.

D. Prosecution History

The '072 patent issued from Appl. No. 11/304,794, filed December 16, 2005. During examination, the Examiner rejected the application claims several

times as anticipated by "Knowbots, Permission Headers and Contract Law" by Henry Perritt ("Perritt") (*see* Ex. 1019). In response, Patent Owner amended the claims to specify the usage rights and a digital work were stored in ***separate*** files, and the recipient computer (*i.e.*, document platform) checks the usage rights before rendering a digital work. *See* Ex. 1004 at 304-315 (Nov. 1, 2007), 5674-5683 (May 23, 2008), 5858-5871 (Oct. 15, 2008). The Examiner allowed the claims, and explained Perritt did not teach a document platform that determines whether the usage rights permit rendering a digital work or the separate storage of a digital work and usage rights. *See id.* at 5918-5919 (Feb. 13, 2009).

E. Claim Construction

The '072 patent claims an effective filing date of November 23, 1994, and expired no later than November 23, 2014. If trial is instituted, the claims must be construed using their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention, in light of the language of the claims, the specification, and the prosecution history of record. IPR2014-00247, Order (Paper 20) at 2-3 (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313-17 (Fed. Cir. 2005) (*en banc*)); *In re Rambus*, 694 F.3d 42, 46 (Fed. Cir. 2012) ("the Board's review of the claims of an expired patent is similar to that of a district court's review"). The '072 patent has a glossary defining many terms used in the claims. Ex. 1003 at 50:5-52:4 (hereinafter "glossary"). These explicit

definitions control the construction of the defined terms, which the Board relid on in construing the meaning of certain terms of the ’072 patent in IPR2013-00133. Those constructions were based on substantial evidence and should be used here.

1. “Digital Document” / “Digital Works”

Each independent claim recites the term “***digital document.***” Ex. 1003 at 52:8-9. A “***digital document***” is “*a digital work having two or more distinguishable parts, where each part contains distinct encapsulated digital information to which is permanently attached a separate usage right that enables independent enforcement of that right for that part of the digital document by a repository (e.g., a ‘document repository’ or a ‘document platform’).*”

None of the applications to which the ’072 patent claims benefit contain the term “digital document”; it only appears in the claims and in the Abstract:

> A method . . . for securely rendering digital documents, including ***storing a digital document*** in a document platform; and ***storing a usage right*** associated with ***the digital document***. . . . The ***digital document comprises plural parts of digital content***. The usage right includes ***plural usage rights respectively associated with each of the plural parts of digital content***. Whether ***one of the parts*** of the digital document ***may be rendered*** by the document platform ***is determined based [sic] a respective usage right***. If the respective usage right allows [it] to be rendered …, the corresponding part…is rendered …

Id. at Abstract. A “composite digital work” is the most logical analog described in

the ’072 patent to a “digital document.” The glossary defines a composite digital work as “[a] digital work comprised of ***distinguishable parts***. ***Each*** of the distinguishable parts ***is itself a digital work which has usage rights attached***.” *Id.* at 50:29-32. Thus, the “composite digital work” is simply an aggregated set of individual digital works. Ex. 1013 at ¶ B119-22. For example, the ’072 patent explains that “rights and fees are additive” (*i.e.*, of the individual rights and fees attached to the individual digital works within the composite digital work).[1] *Id.* at 17:64-66. As defined, each part of a “composite digital work” has a separate usage right attached to it, which enables each right to be enforced independently for each part of the work to which it is attached. *Id.* at 17:64-66, 8:46-51 (“Each of the articles and photographs may represent a node . . . ***controls, i.e. usage rights***, ***may be placed on each node*** . . . . enabling control and fee billing to be associated ***with each node***”).

The description of a “***digital document***” in the Abstract indicates it is a type of “composite digital work.” This is because: (i) it contains two or more

---

[1] The glossary defines digital “content” as “the digital information (i.e. raw bits) representing a ***digital work***.” *Id.* at 50:33-35, 6:3-5. It defines a “***digital work***” as being “any encapsulated digital information” to which “usage rights and fees” are attached. *Id.* at 50:61-63, 6:27-37, 8:52-59.

"distinguishable" parts, (ii) it attaches different usage rights to each of the parts, and (iii) it independently enforces the different usage rights attached to each part. *Id.* at 50:29-32; Ex. 1013 at ¶ B122. To enable this functionality within the '072 patent scheme, each of the constituent parts of the "digital document" must be a "digital work" to which is permanently attached a ***separate*** usage right. *Id.* at 50:29-32 ("[e]ach of the distinguishable parts is itself a digital work which has usage rights attached"), Abstract ("***plural*** usage rights [are] ***respectively associated*** with ***each of the plural parts*** of digital content"). The digital document and its constituent parts must have permanently attached usage rights, and can only be stored in, transferred among or used by repositories. Ex. 1013 at ¶ B121-23, B110-111. Ex. 1003 at 10:49-50; 6:18-21 ("the usage rights … will ***always remain*** with a digital work"), 6:31-37, 8:46-51, 17:65-66.

Attached usage rights and mandatory use of repositories are key elements of the '072 patent scheme. Ex. 1013 at ¶ B108-B111; Ex. 1003 at 6:22-32, 6:13-16, 10:49-50. Thus, if a digital document or its constituent parts are disseminated without their attached usage rights or transmitted outside of a repository, the "content genie [is] out of the bottle," preventing the '072 patent's central purpose of preventing unapproved uses or transfers of the digital document or its individual parts. Ex. 1003 at 6:28-37. The '072 patent thus only describes repositories storing, copying or distributing the information representing a work in the form of

a "digital work," and describes no processes where a digital work or a work is transmitted by or via devices that are not repositories. Ex. 1013 at ¶ B111-113; Ex. 1003 at 6:45-65 ("[t]he digital work remains securely in Repository 1 … [then] repository 1 transmits the digital work to repository 2"); 6:40-43 ("a creator creates a digital work . . . determine[s] the appropriate usage rights and fees, attach[es] them to the digital work, and store[s] them in Repository 1"), Fig. 1, 6:34-36. Because a "digital document" is a "digital work," it can only be used by or transferred between "repositories" and the individual usage rights permanently attached to each part of the digital document are necessarily enforced by repositories. Ex. 1013 at ¶ B116-123, B104-115.

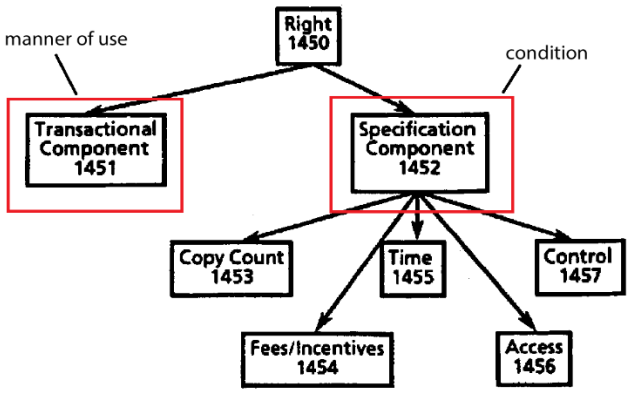
2. "Usage Rights" and "Manner of Use"

Each independent claim recites the terms "***usage rights***" and "***manner of use***." The glossary defines "***usage rights***" as "[a] ***language*** for defining ***the manner*** in which a digital work may be used or distributed, ***as well as any conditions*** on which use or distribution is premised." Ex. 1003 at 51:65-67. A "***usage right***" thus is a data construct that consists of "*statements in a language defining one manner in which the digital work may be used or distributed, and optionally, one or more conditions on which use or distribution is premised, and is permanently attached to one digital work.*" Multiple usage rights may be attached to one digital work (each specifying a particular manner of use and associated

conditions), but the converse is not true – one "usage right" cannot be attached to multiple digital works. Ex. 1013 at ¶ B54-55. "Usage rights . . . are attached to [a] digital work." *Id.* at 50:62-63, 6:16-17("[a] key feature of the present invention is that usage rights are permanently 'attached' to the digital work.").

The '072 patent shows each usage right will include a "***manner of use***" (*i.e.*, one of a number of actions defined in the usage rights language that can be taken with the digital work) and may include, as a distinct element within the usage right, one or more optional "***conditions***" governing that manner of use. *Id.* at 18:66-19:5, 51:64-67, 18:9-16. The '072 patent shows each "statement" in the usage rights language specifies one "right code" and optionally may specify one or more "conditions" on exercising that right code. *Id.* at 18:66-19:5. Figure 14 depicts each "usage right" (1450) having one "transactional component" (1451) and a "specifications component" (1452) with multiple "conditions" (1453-1457) within it. *Id.* at 18:5-6. The "transactional ***component*** 1451 corresponds to a particular way in which a digital work may be used or distributed," (*id.* at 18:9-10), while the "specifications ***components*** 1452 are used to specify conditions which must be satisfied prior to

Figure 14



the right being exercised or to designate various transaction related parameters," (*id.* at 18:13-16). *Id.* at 9:50-55, 18:11-19, 10:6-33.

The '072 patent shows a particular "manner of use" within a "usage right" is implemented as a value (the "right code") representing the action that can be taken with the digital work. "Each usage right ***must specify a right code***," (*id.* at 19:1-4), which corresponds to the particular "use or distribution privilege[] embodied by the right," such as "COPY or PRINT," (*id.* at 18:6-8). *See also id.* at 9:50-57 ("each right will have a right code field 1001 and status information field 1002"), 19:1-5, Fig. 10, 17:43-50, 17:54-56, 19:15-21 ("the grammar provides a catalog of possible rights that can be associated with parts of digital works"), 18:59-61 ("The ***set of rights*** attached to a digital work ***define how that digital work may be transferred, used, performed or played***."); Ex. 1013 at ¶ B38. Examples of "manners of use" (actions) include "play," "copy," "transfer," "backup," and "install." Ex. 1003 at 19:15-20:28. The "manner of use" specified by the value of the right code in any particular instance of a digital work is enforced by the repository when it reads that right code value and interprets it using the usage rights language. *Id.* at 17:47-56.

"Conditions" are implemented as distinct elements relative to the "manner of use" within the usage right. *Id.* at 6:11-14. Thus, the same element within the "usage right" cannot be both a "manner of use" and a "condition" (*e.g.*, the "right

code" does not specify a condition). Ex. 1013 at ¶ B43, B49. The '072 patent also explains each condition is designed to limit a particular manner of use, rather than applying more generally to a digital work as a whole. *See* Ex. 1003 at 20:62-64 ("The copy-count is associated ***with each right***, as opposed to there being just a single copy-count for the digital work."). While a "manner of use" is a mandatory element of a "usage right," a "condition" is not. *Id.* at 19:2-4 ("Each right may also ***optionally*** specify conditions which must be satisfied before the right can be exercised.").

"Usage rights" also are distinct from data within a digital work or provided independently that is used by repositories to enforce usage rights. As the '072 patent explains, "[t]he enforcement elements of the present invention are embodied in repositories." Ex. 1003 at 6:22-23. Thus, data constructs such as encryption keys, digital certificates, and digital signatures used by the repository to control access to a digital work or data within are not "usage rights." IPR2013-00138, Paper 54 at 38:18-39:1. Per the '072 patent, a repository interprets information within "usage rights" to determine ***which*** actions can be taken with the work, while enforcement elements (*e.g.*, the decryption keys, digital certificates, digital signatures) are used to decrypt and/or authenticate instances of digital works. Ex. 1003 at 6:9-12 (usage rights "***define how a digital work can be used*** and ***if it can be further distributed***."), 17:47-50.

Thus, each "***usage right***" will take the form of data permanently attached to a particular copy of a digital work that specifies: (i) one "manner of use" out of a defined set of manners of use defined in the usage rights language that may be taken with that copy of the digital work and (ii) optionally includes one or more conditions associated with exercising that manner of use. These data contain the "statements" of the language or data encoding such statements, and they are distinct from data that is used by a repository to enforce the "usage right" (*e.g.*, encryption keys, digital certificates, digital signatures). Ex. 1013 at ¶ B61.

Finally, a "***manner of use***" is "*a defined way of using or distributing a digital work (for example, PLAY, COPY, or PRINT), as distinct from conditions which must be satisfied before that way of using or distributing the digital work is allowed.*" Ex. 1013 at ¶ B59.

3. "Repository"

Each challenged claim recites one or more forms of a "***repository***" (*e.g.*, a "document repository" or "document platform"). A "***repository***" is "*a trusted system in that it maintains physical, communications and behavioral integrity, and it supports usage rights by controlling which actions can be taken with a digital work by using information in that work's usage rights.*" Ex. 1003 at 6:22-23, 51:34-38; *see* IPR2013-00133, Paper 61 at 9 (July 1, 2014) ("ZTE Final Dec."). In earlier proceedings involving the '072 patent, the Board adopted the glossary

definition of the term "repository" – "a trusted system in that it maintains physical, communications and behavioral integrity" and it supports usage rights. *Id.* at 9; Ex. 1003 at 51:34-38. The Board explained a repository must possess three types of integrity: (i) "***physical integrity***" (*i.e.*, a repository "'prevent[s] access to information by a non-trusted system'") (ZTE Final Dec. at 10-11; Ex. 1003 at 12:1-26); (ii) "***communications integrity***" (*i.e.*, a repository "'only communicates with other devices that are able to present proof that they are trusted systems, for example, by using security measures such as encryption, exchange of digital certificates, and nonces'") (*id.* at 11-12); and (iii) "***behavioral integrity***" (*i.e.*, a repository "'requir[es] software to include a digital certificate in order to be installed in the repository.'") (*id.* at 12-13).

Certain additional clarifications are warranted regarding "digital certificates" and "supporting usage rights." For example, the Board found "communications" and "behavioral" integrity to require use of "digital certificates." *See* ZTE Final Dec. at 12-13 (a repository will only transfer content to devices that are "able to present proof that they are trusted systems"); Ex. 1003 at 7:37-39 ("Identification certificates are the means by which a repository is identified as 'trustworthy'."). The glossary defines a digital certificate (*i.e.*, "Identification (Digital) Certificate") as "[a] ***signed*** digital message that attests to the identity of the possessor." Ex. 1003 at 51:1-4; *see id.* at 26:34-37. This is consistent with how a person of skill

would understand that term: a digital certificate is a digitally signed message that binds an identity to a public key. Ex. 1017 at 170; Ex. 1013 at ¶ B70-71. Digital certificates are issued by a trusted certificate authority, whose digital signature on the certificate attests that the entity identified in the certificate registered the identified public key. Ex. 1013 at ¶ B71.

The '072 patent explains that, to ensure behavioral integrity, software applications distributed as "content" must be "certified" by distributing a digital certificate with the software. Ex. 1003 at 12:47-48 (the digital certificates provide "proof of [the software's] certification"), 12:52-56 ("If the ***digital certificate*** cannot be found ***in the digital work . . .*** then the software cannot be installed."; 41:63-42:6 (showing a "digital certificate" used to certify "a digital work as ***runnable software*** on a repository"); *see* ZTE Final Dec. at 19-21. A person of skill would understand that "certifying" a digital work necessarily involves using a digital signature created by the entity identified in the certificate (*e.g.*, by encrypting a digest of the software file with its private key). Ex. 1013 at ¶ B73; Ex. 1003 at 42:46-51 (explaining that a repository validates an encrypted "tamper-checking code," *i.e.*, a digital signature, associated with the software). This conventional digital signature technique is what enables a repository receiving the software to ***verify*** the ***source*** (the entity identified in the certificate) and ***integrity*** (that the software had not been modified since being signed). Ex. 1013 at ¶ B74-

76. Otherwise, any entity could simply copy and append a digital certificate to the software, making it appear as if the software was certified. *Id.*

Each repository must be able to support usage rights – "[t]he enforcement elements of the present invention are embodied in repositories." Ex. 1003 at 6:22-23. To do this, repositories interpret data in the usage right to determine what actions can be taken with the digital work. *Id.* at 17:47-50 ("Usage rights statements are interpreted by repositories and are used to determine what transactions can be []carried out for a digital work and [the] parameters for those transactions."); Ex. 1013 at ¶ B62, B88. Without repositories, usage rights are incapable of controlling the use or distribution of the digital work; this is why every illustration in the '072 patent of digital works being transferred or rendered shows a repository storing, transferring, or rendering the digital work. *Id.* at ¶ B53, B64; Ex. 1003 at 6:38-7:2.

4. "Document Platform"

Each independent claim recites the term "***document platform***." A "document platform" is "*a repository that is able to receive, transmit, store and render digital documents*." Ex. 1013 at ¶ B142-145. The Abstract (the only part of the '072 patent that mentions a "document platform"), explains a "document

platform" stores and renders a "digital document."[2] Each claim also specifies that a "document repository" ***transmits*** a digital work ***to the document platform*** and the "document platform" ***retrieves*** and ***stores*** digital documents (*i.e.*, a digital work) and usage rights associated with such digital documents. Ex. 1003 at 52:54-67. Claims 1 and 18 specify the document platform ***enforces*** usage rights.

Based on the role and functions performed by a "document platform," it is necessarily a "repository." Ex. 1013 at ¶ B142-145. In the '072 patent scheme, only repositories transmit, store, and render digital works because they are the only devices that are shown as being "trusted" and which can "enforce" usage rights. Ex. 1003 at 11:58-61 ("Many of the powerful functions of repositories . . . are possible because they are trusted systems."), 6:35-37 ("the digital work genie only moves from one ***trusted*** bottle (***repository***) to another"), 7:6-8 ("It is ***fundamental that repositories . . . enable*** secure and ***trusted communications.***"), 6:23-24 ("[t]he enforcement elements of the present invention are embodied in repositories").

The '072 patent uses the term "platform" in only three instances. Each instance is consistent with the "platform" being a "repository." In a section entitled "***Repository*** Transactions," it states that "[t]ransactions occur between two

[2] Petitioner expressly reserves its right to contend the claims are indefinite under § 112 in other proceedings.

repositories (one acting as a server), between a repository and a ***document playback platform*** (e.g. for executing or viewing)." *Id.* at 26:25-27; *see id.* at 10:52-54. Then, in a "loaning" example, a digital work is loaned from a server to another device (a "requester ***platform***") to permit its use. *Id.* at 35:36-44. Third, the '072 patent describes an "Install transaction," which "is a request to install a digital work as runnable software ***on a repository***." *Id.* at 41:64-42:40. In this process, "[i]n a typical case, the ***requester repository*** is a ***rendering repository*** and the software would be a new kind or new version of a player." *Id.* As the '072 patent observes:

> The ***requester*** [i.e., the "requestor repository"] retrieves the instructions in the compatibility-checking script and follows them. If the software is not compatible with ***the repository***, the installation transaction ends with an error. (***This step checks platform compatibility***.)

Id. at 42:25-29. The use of "platform" interchangeably with "rendering repository" plainly indicates it must be a ***repository***. *See* Ex. 1013 at ¶ B143-144. It also shows the '072 patent envisions particular ***types*** of repositories, such as a "***rendering***" repository, which, in addition to being a "repository," can "render" content stored in it. *See* Ex. 1003 at 51:23-26 ("A special type of repository which is typically coupled to a rendering system. The rendering repository will typically be embodied within the secure boundaries of a rendering system.").

Logically, then, a "document platform" is a "platform" that can be used with "digital documents." The "document platform" must be at least a repository because, as the claims specify, the "document platform" performs ***repository*** transactions (*e.g.*, "***retrieving*** … a digital document and at least one usage right . . . ***from a document repository***, …***storing*** [them]…, ***determining***, by the document platform, whether the digital document may be rendered"). *Id.* at Claim 1; Ex. 1013 at ¶ B142-B145. The distinct language used ("document platform") simply reflects that it is a repository for digital documents. *Id.*

IV. Analysis of the Patentability of the Claims of the '072 Patent

As noted in § III.B.2, the '072 patent has three independent claims, and each defines a method for "*securely rendering digital documents*" with minor variations of the same operative steps. Ex. 1013 at ¶ E182-191.

Rosen in view of Hartrick suggests methods and systems that would have rendered the '072 claims obvious to a person of ordinary skill before 1994. Rosen teaches techniques for exchanging digital content (*e.g.*, software, books, or movies) using trusted devices with tamper-resistant processors, permanently attaching usage information to each copy of content, and using digital certificates to initiate secure channels. *See* Ex. 1013 at ¶ E1-9. Rosen explains that content is distributed in encrypted form along with a decryption ticket that has a "Usage" field that specifies "restrictions on usage of the electronic object," but does not elaborate

how those restrictions are specified or enforced. To implement Rosen's system, a person of skill would turn to known techniques, such as those in Hartrick, which describes techniques for controlling the use and distribution of digital books encoding each book with specialized markup language (SGML) tags. A person of skill would have recognized these two systems could be readily integrated and combining them would improve the functionality of both systems (e.g., by providing more granular control over distributed content and added security).

A. The Rosen System

U.S. Patent No. 5,557,518 to Rosen (Ex. 1020) was filed on April 28, 1994 and is prior art to the '072 patent under 35 U.S.C. § 102(e). Ex. 1020; Ex. 1013 at ¶ B204. The operation and features of Rosen are explained below and in further detail in Ex. 1013 at ¶ E1-69, A89-90, A159-160.

1. Overview of Rosen

Rosen describes a scheme for facilitating the exchange and rendering of digital content (*e.g.*, software, movies, and other electronic content). Ex. 1020 at 1:5-11, 4:54-64, 8:28-31. Merchants and customers use "transaction devices" to create, find, sell, purchase, and render digital content. *See id.* at 7:65-8:53, § IV.A.3. Transaction devices are "trusted systems" - each contains a "trusted agent," which is a physically secure, tamperproof module that enforces security protocols and securely stores key information. *Id.* at 1:5-15, 2:12-14, 4:4-39, 7:65-

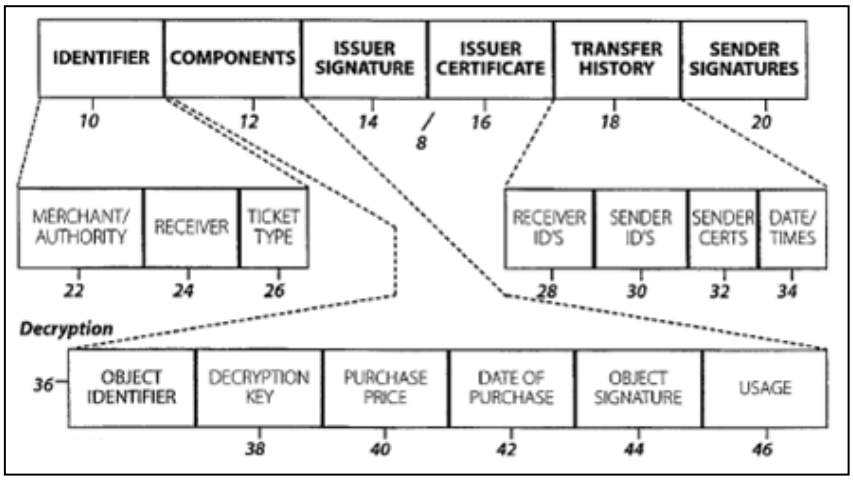
8:7; *see* § IV.A.3. A merchant transaction device can be part of a "merchant network," which is a distributed system that includes content servers, merchant transaction devices, and trusted authorization servers. *See id.* at Fig. 5, 10:19-29; Ex. 1013 at ¶ E53-56.

2. Electronic Objects and Tickets

In the Rosen scheme, digital content is stored in an encrypted file called an "electronic object." Ex. 1020 at 4:41-44, 4:54-5:3, 6:3-4. Each electronic object consists of a cleartext header containing information about the content (including an "object identifier") and a body containing the encrypted content. *Id.* at 5:63-6:4; Ex. 1013 at ¶ E21, E120. When purchased, a unique "decryption ticket" is permanently associated with each electronic object, without which its content cannot be accessed. Ex. 1020 at 5:59-6:13, 4:54-55 ("A decryption ticket is always associated with a particular encrypted electronic object."), 4:60-63, 4:55-5:3. A customer can subsequently transfer the encrypted electronic object to other transaction devices, but it must be accompanied by the corresponding decryption ticket. *Id.* at 7:42-61, 25:64-65; *see id.* at 7:29-61.

Figure 2 of Rosen illustrates a decryption ticket, and shows it has various fields. The "Object Identifier" field (36) uniquely ties the ticket to the electronic object using the object identifier in the object's header. *Id*. at 5:64-66. The "Usage" field (46) specifies "restrictions on usage of the electronic object." *Id.* at

6:12-13. The "Decryption Key" field (38) contains the key to decrypt the object. *Id.* at 6:3-4. The "Object Signature" field (44) contains the electronic object's digital signature, signed by the entity that issued the ticket. *Id.* at 6:7-12. The decryption ticket itself is signed by the issuer (in the "Signature 14" section). *Id.* at 7:29-61. The decryption ticket also contains the issuer's digital certificate ("Issuer Certificate 16"), which, together with the signature fields (16 and 44), is used to check the source and integrity of the object. *Id.* at 7:29-61.



Rosen describes other types of "tickets" that are used for different purposes and are not associated with electronic objects. *Id.* at 4:52-5:23. For example, "[a] credential ticket [that] identifies the 'owner' and permits specific privileges." *Id.* at 5:4-5, 5:34-35, 6:14-25. As Rosen explains:

> All [merchant transaction devices] contain a credential identifying the owner/merchant (e.g., NYNEX, Ticketron, etc.). Such merchant credentials may, for example, be issued by a merchant identification authority controlled by the Trusted Agency. On the other hand, customer credentials held by [customer transaction devices] may include driver's licenses or credit cards issued by various identification authorities.

Id. at 18:5-13, 5:5-7, 26:44-54. These tickets are used as proof of authorization in various contexts. *See* § IV.A.4; Ex. 1013 at ¶ E27.

3. Transaction Devices and Trusted Agents

Participants in the Rosen scheme must have a "transaction device," which is a computer system that includes a trusted agent, host processor, and money module. *Id.* at 7:65-8:7, 8:22-34, 25:63-26:39; *see id.* at 8:3-7 ("customer transaction device" is a "CTD" and "merchant transaction device" is a "MTD"). Each transaction device has "transaction applications" installed on it, which are software programs for finding, exchanging, or rendering content:

> Transaction Applications 130 may perform a variety of tasks. . . [A] transaction application may provide for the interim storage of electronic objects and possibly execute objects. In order to execute an electronic object, there may be additional object processors depending on the type of electronic object (e.g., movie, book, multimedia game, etc.). In short, a transaction device 122 contains all the processes to choose, buy and possibly use electronic objects, credentials, and other tickets 8, or the processes to sell the same.

Id. at 8:22-34, 7:65-8:7. A person of ordinary skill would understand that in order to render content for a user, the transaction device must first receive a request from a user to render that content. *Id.* 8:35-40 (describing the "Human/Machine Interface"); Ex. 1013 at ¶ E17, E20.

Rosen transaction devices contain a "trusted agent," which is a tamper-

resistant module that contains a processor, memory, and communications interfaces. Ex. 1020 at Fig. 4A, 4:4-39 ("A trusted agent is a combination of hardware and software components. It is tamperproof and contains secure protocols . . ."), 9:1-15. The memory stores software that provides security services, such as a session manager (for initiating and managing communications), a security manager (for managing digital certificates), and cryptographic support functions (for securely encrypting and decrypting data). *Id.* at 9:1-15, 4:4-39, 11:6-24. Each trusted agent has a unique identification number assigned to it when it is manufactured. *Id.* at 11:6-30; *see id.* at 10:41-13:14.

Each trusted agent is configured with software modules that support functionality specific to a merchant, a customer, or another trusted entity. *See id.* at 4:34-36, 8:57-65, Figs. 4A-4D. The merchant's trusted agent ("MTA") is configured to generate new decryption tickets for delivery to a customer. *Id*. at 9:60-61, 18:66-19:8. The customer's trusted agent ("CTA") has a memory that contains space for storing decryption tickets for electronic objects. *Id.* at 9:60-61 ("A Ticket Holder function 148 . . . stores and retrieves tickets 8 in a CTA 2."), 19:37-39, 24:52-55, Fig. 15B; Ex. 1013 at ¶ E9, E15, E59. A customer cannot access an electronic object's content unless the CTA has the decryption ticket:

> The transferred electronic object is cryptographically secure from inspection and use by the receiving customer or any other third party unless they have access to the decryption ticket. The decryption ticket,

> in turn, is the 'property' of the CTA and may only be used upon successful completion of the purchase transaction.

Ex. 1020 at 4:54-5:3; *see id.* at 4:47-50. Decryption tickets are stored within the trusted agent, (*id.* at 9:60-61, 4:65-5:3, 5:55-6:2, 24:52-55), while electronic objects can be stored in the transaction device's memory because they are encrypted, (*id.* at 23:16-22). To access an electronic object's content, a transaction application sends the unique identifier from the object's header to the trusted agent, which uses the information to retrieve the object's decryption ticket. *Id.* at 9:60-61, 24:52-55 ("Ticket Holder A sends the decryption key and the electronic object identifier from the decryption ticket to a host transaction application for its use in decryption of the electronic object"); Ex. 1013 at ¶ E9, E19, E21.

4. The Trusted Agency Certificate Authority

A central feature of the Rosen scheme is that a trusted agent will only communicate with another trusted agent that has a digital certificate issued by the "Trusted Agency." Ex. 1020 at 37:18-49. Each trusted agent must have a digital certificate from this authority to identify itself as trustworthy. *Id.* at 11:6-30. The Trusted Agency is a system of servers that act as a certificate authority, which was known in the art as a system for distributing digital certificates and other related data. Ex. 1013 at ¶ A159-160, E28. The trusted servers "are tamper-proof processors" and two of their primary functions are "certification of trusted agents" (*i.e.*, issuing digital certificates) and "distribution of untrusted lists." Ex. 1020 at

10:45-50. Untrusted lists contain the id numbers of compromised devices; each agent checks these lists when validating a digital certificate and will reject the digital certificate if the owner's id number is on the list. *Id.* at 12:48-55.

To obtain a digital certificate, the trusted agent generates a public key; it then registers the public key and its unique identification number with a trusted server. *Id.* at 11:14-25. The resulting digital certificate expires periodically, at which point the trusted agent must recertify. *Id*. at 12:14-33, 15:14-20. To recertify, a trusted agent sends a request to a trusted server for a new digital certificate. *Id.* at 12:14-33, 15:15-29. The trusted server will verify the trusted agent's expired certificate and will check its id number against the untrusted list. *Id.* at 15:30-45. If the requesting agent can still be trusted, the trusted server will issue it a new digital certificate. *Id.* at 15:45-57, 16:60-17:7, 17:16-39. If a trusted agent has an expired certificate or if its id number is on the untrusted list, it cannot interact with or exchange and receive content from other trusted agents. *Id.* at 15:21-16:16, 17:61-63, 23:12-22, 26:13-17, Figs. 12A-B, 25A, 38A-E.

5. Secure Transaction Protocols

Each trusted agent in the Rosen scheme contains software for performing several secure protocols that allow trusted devices to communicate and exchange electronic objects and tickets. *Id.* at 4:4-39 ("A trusted agent . . . contains secure protocols . . . [and] neither party can modify [them] to the disadvantage of the

other party."). These include an "Establish Session" protocol, a purchase transaction protocol, and an acquire credential protocol.

The "Establish Session" protocol allows trusted agents to "establish[] a cryptographically secure session" with other trusted agents, which is a prerequisite to the transfer of any electronic objects and decryption tickets. *Id* at 2:13-15, 17:61-67, 26:8-39, Figs. 12A & 12B (step 408). By exchanging a series of messages according to the protocol, a session can be established between any two trusted agents, such as two CTAs (*id.* at 26:13-14), a CTA and an MTA (*id.* at 17:61-63), or a CTA (or MTA) and a Trusted Agency server (*id.* at 15:21-23). *See id.* at 37:18-38:20, 13:18-34; Ex. 1013 at ¶ E40-E51.

To initiate a session between two agents, for example for an MTA to initiate a session with a CTA, the MTA first sends its digital certificate to the CTA. Ex. 1020 at Fig. 12 (step 408), 37:29-30; Ex. 1013 at ¶ E48-E51. The CTA validates the certificate (Ex. 1020 at 37:34-41), and then it sends a message to the MTA containing (1) the CTA's digital certificate, (2) a first random number, (3) a first "verification message" (which is "a random number used [] to protect against message replay," *id.* at 15:49-51), and (4) the date and time. *Id.* at 37:30-49. The MTA validates the CTA's digital certificate, and then it sends a message to the CTA containing (1) the first verification message, (2) a second random number, (3) a second verification message, and (4) the date and time. *Id.* at 37:50-38:2. The

CTA verifies the first verification message is correct and uses the two random numbers to create a session key. *Id.* at 37:64-65, 38:2-8. The CTA then returns the second verification message to the MTA. *Id.* at 38:12-15. The MTA verifies the second verification message is correct, generates a session key, and then the session and secure channel are established. *Id.* at 38:14-20. During this process, if either agent detects a problem with the other's digital certificate, the session will terminate. *Id.* at 37:29-61. Any data transferred between the trusted agents during the session will be encrypted with the session key. *See id.* at 17:61-63.

The Rosen purchase transaction protocol allows a customer to purchase content (*i.e.*, an electronic object plus decryption ticket) from a merchant using a standard process. *See id.* at 17:41-24:63. After locating desired content on a merchant's content server, the customer's transaction device sends a purchase request to the merchant's transaction device. *Id.* at 8:22-34, 17:49-60. Each transaction device then passes the process to its trusted agent. *Id.* at 17:55-60. The CTA establishes a session with the MTA using the "Establish Session" protocol discussed above. *Id.* at 17:61-67, 37:18-38:20. After the session is established, the MTA sends its merchant credential ticket to the CTA to prove it is a merchant. *Id.* at 18:13-16; *see id.* at 18:5-12, 5:4-7. The CTA validates the credential ticket (if invalid, it terminates the session). *Id.* at 18:17-34. The MTA then prepares a new electronic object for delivery by obtaining the content from a merchandise server,

"encrypt[ing] the electronic object with [a] random key, and [] digitally sign[ing] the encrypted electronic object with [its] private key []." *Id.* at 19:3-6. The MTA creates a new decryption ticket containing the random key, usage information, and several digital certificates and signatures. *Id.* at 19:6-8; *see* § IV.A.2. The MTA transmits the encrypted electronic object and decryption ticket to the CTA through the secure channel. *Id.* at 17:49-60, 18:66-19:14, 23:13-22.

The CTA "verifies the encrypted electronic object's signature using [the MTA's] public key . . . , and [i]f the signature is incorrect, then the transaction is aborted." *Id.* at 19:17-20. The CTA performs additional validations on the object and decryption ticket, (*id.* at 19:20-35), and if everything is valid, the CTA "sends the decryption ticket to Ticket Holder A for storage," (*id.* at 19:35-39). The encrypted electronic object can be stored in the transaction device's memory as it is inaccessible without the decryption ticket, and the CTA will not allow access the decryption ticket until the transaction is complete. *Id.* at 19:40-43 ("the merchandise is inaccessible to the customer due to its encryption and/or its storage within his trusted agent"), 23:16-21, 4:65-5:3. Storage of the ticket and object are "provisional" until the transaction is committed. *Id*. at 2:17-19, 23:4-6.

Next, the CTA transmits a payment credential ticket to the MTA to show it can pay for the electronic object. *Id.* at 5:4-7, 19:46-49, 24:21-29; § IV.A.2. If the credential is valid and the payment can be processed, the MTA will return an

authorization message. *Id.* at 24:29-49. The trusted agents will then commit the transactions. *Id.* at 22:65-23:9, 24:41-49. The CTA permanently stores the decryption ticket, and passes the electronic object to the transaction device for storage and use. *Id.* at 23:1-9, 23:41-51.

Rosen explains "the order of exchanging electronic merchandize and money may be reversed" so that the CTA first sends its payment credential ticket to the MTA; the MTA validates the credential ticket, and if valid, transmits the electronic object and decryption ticket to the CTA. *Id.* at 19:13-39, 22:20-67, 23:23-40, 23:52-61; Ex. 1013 at ¶ E62.

Rosen also describes a protocol for acquiring a credential ticket. Ex. 1020 at 26:44-27:30, Fig. 26. Both CTAs and MTAs can acquire credentials from a special trusted agent, an Identification Authority trusted agent ("ATA"), using the same process. *See id.* at 26:44-49, 26:49-53 ("The credentials can be . . . acquired remotely if the trusted agent 120 already contains credentials for proof of identity. . . ."). For example, for a CTA to obtain a credential ticket, the CTD sends a request to the Identification Authority's transaction device. Ex. 1020 at 26:44-27:30. The request will be passed to the ATA, which determines if the request should be granted. *Id.* at 26:57-59, 27:53-59. If so, the ATA will use the "Establish Session" protocol to initiate a session with the CTA, create a new credential ticket, and then transmit the ticket to the CTA. *Id.* at 27:5-14, 27:62-65.

B. Overview of Hartrick (Ex. 1021)

European Patent No. EP 0 567 800 to Hartrick ("Hartrick") (Ex. 1021) was published on November 3, 1993, and is prior art to the '072 claims under 35 U.S.C. § 102(b). Ex. 1021; Ex. 1013 at ¶ B206. The operation and features of the Hartrick scheme are explained below and in Ex. 1013 at ¶ E70-103.

1. Overview

Hartrick describes a technique for controlling the use and distribution of "softcopy" (*i.e.*, digital) books. Ex. 1021 at 1:3-8, 5:19-38. Included with each softcopy book is security and royalty information that specifies whether it can be reproduced and any associated fees. *Id.* at 1:3-8, 3:12-22, 3:28-32, 5:48-52. The security and royalty information is enforced by a royalty payment program on the user's computer, which intercepts requests from the user to store, copy, print, and transmit a book or portions thereof. *Id.* at 6:9-22, Fig. 1. The royalty payment program prevents the user from performing a requested operation unless it is permitted and the user has purchased the right to perform it. *Id.* at 16:10-21. If the requested operation is permitted and paid for, a separate softcopy book reading program renders the book on end-user's computer. *Id.* at 6:1-9.

Hartrick explains each softcopy book is a "structured document" formatted using SGML, a markup language that uses "tags" to describe each "element" (*e.g.*, component) of a document. *Id.* at 4:25-36, 5:3-8, 5:42-47. For example, the

"[bk]" tag is used to denote a book's title ("[bk] Book Title [/bk]") and the "[p]" tag denotes a paragraph of text ("[p] Paragraph of text…[/p]"). *Id.* at 1:28-39, 4:38-42, 9:41-49, 11:37, 12:45. The softcopy book reading program uses these tags to, *e.g.*, format the output displayed to a user. *Id.* at 1:12-16, 2:21-28.

2. Specialized Security and Royalty Markup Tags

Hartrick teaches that specialized SGML tags are incorporated into each book, which are interpreted by the royalty payment program to determine how the book can be used and whether the user needs to pay a royalty before taking certain actions. *See id.* at 3:53-58, 10:1-14. Hartrick explains that two types of tags, security tags and royalty tags, allow authors and distributors to control end-users' ability to, *e.g.*, "print[] pages of a structured document," "writ[e] [] a structured document into bulk storage," and transmit via "telecommunication [] soft copies of a structured document." *Id.* at 5:24-26, 30-32, 35-37. The tags can be placed "within the structured document text of the book or in a royalty payment information file which accompanies the book." *Id.* at 5:48-52.

Hartrick teaches that "security tags" are "special structured document tag[s]" that specify how the book can be used, and the royalty payment program interprets these tags to prohibit certain operations on the book. *Id.* at 3:28-32, 3:48-4:9. For example, if a book contains the "Do Not Copy" tag, the royalty payment program will permit a user to view the book, but inhibit printing, copying, or transmitting it.

Id. If a user requests to print a book that contains this tag, then any requested "printing operation[s] will be aborted in response to the [tag's] presence." *Id.* at 3:53-57. A book can contain other security tags, such as a "Do Not Distribute" tag, which prevents the document from being transmitted (*id.* at 3:28-32, 4:4-9), and a "copyright" tag that will cause every page of the displayed document to contain a copyright notice, (*id.* at 3:33-40, 50-53). *See* Ex. 1013 at ¶ E82-85.

Each softcopy book can include "royalty tags" that allow an author or publisher to specify different fees that must be paid to reproduce the book or any part of the book (*e.g.*, a different fee for each chapter). Ex. 1021 at 5:42-47, 10:1-14, 10:41-54, 11:46-12:36; Ex. 1013 at ¶ E87-90. In certain embodiments, Hartrick depicts a general "royalty" tag as regulating any type of "reproduction" of a book (*e.g.*, printing, copying, ***and*** transmitting). *See* Ex. 1021 at 11:46-12:36. Hartrick also shows separately regulating individual actions a user can take with a softcopy book (*e.g.*, print, copy, transmit) using the royalty tags. *Id.* at 5:24-26, 30-32, 35-37; 6:9-22; 10:7-18. Hartrick also separately defines in the claims methods for controlling different rights, specifying a publisher can separately authorize each of printing, copying, or transmitting a book. *Id.* at 21:56-22:3, 22:7-10 (print); 22:34-38, 22:42-45 (copy); 23:13-14, 23:21-24 (transmit). A person of skill would have understood the Hartrick description as teaching different royalty tags can be used to specify fees for the different operations being

taken by a user with a softcopy book, as it uses a distinct tag for each action (*e.g.*, printing, copying, and transmitting) regarding the book (*e.g.*, "[print-royalty]" and "[transmit-royalty]"). *See* Ex. 1021 at 5:19-38, 6:9-22, 10:7-18; Ex. 1013 at ¶ E91-96, E85-87.

3. Enforcement

The rights and restrictions specified in the specialized SGML tags of the Hartrick scheme are enforced by a royalty payment program that runs on each end-user's computer. Ex. 1021 at 6:9-22, Fig. 1. The royalty payment program intercepts requests to access or use books and will not permit the requested operation unless the security tags permit the operation (*id.* at 3:30-32, 3:53-4:9) and any fees specified by the royalty tags have been paid (*id.* at 15:34-40, 16:10-21, 20:1-21). Hartrick explains:

> If the user enters a command to copy the book onto a writable storage medium such as a magnetic disk or to print a hardcopy of the book with a printer or to transmit a copy of the book over a modem, the royalty payment program intercepts the copying command and suspends the copying operations.

Id. at 6:9-19; *see id.* at 3:48-4:9, 10:7-18, 15:23-33. If the user has not yet paid the fee, "the user must select the option of paying a royalty to the publisher before the royalty payment program permits a copy of the book to be made." *Id.* at 6:19-22. The royalty payment program will then send a request to the publisher for

authorization. *Id.* at 15:34-40, 15:53-16:9.

The publisher's server runs a royalty billing program that processes authorization requests from end-users. *Id.* at Figs. 2 & 9, 16:10-33, 6:34-7:10. If the server determines a user can pay for the requested operation, it will return a digitally signed "authorization message" to the user that indicates that the requested operation is allowed. *Id.* at 16:10-21, 16:26-32, 17:18-26, 18:46-19:16. The authorization message includes information specifying which operation (*e.g.*, print or transmit) the user may take (*id.* at 22:7-10, 42-45; 23:21-24) and may include restrictions such as page ranges (*id.* at 16:34-37, 20:5-8, 20:31-35). Only after the user obtains authorization will the royalty payment program permit the requested action to proceed. *Id.* at 16:18-21, 20:5-17.

C. A Person of Ordinary Skill Would Have Found It Obvious to Implement Rosen's Scheme Using Hartrick's Techniques

Rosen describes a system for securely distributing electronic objects from merchants to customers. *See* § IV.A; Ex. 1020 at 1:5-11, 4:54-64, 8:28-31. Rosen explains the electronic object's decryption ticket contains a "Usage" field specifying "restrictions on usage of the electronic object." Ex. 1020 at 6:12-13; *see* § IV.A.2. Rosen does not explicitly describe the format of the usage restrictions, or that they can be implemented using statements in a usage rights language.

A person of ordinary skill would have recognized the data in the "Usage"

field in Rosen has the same role as the security and royalty tags have in the Hartrick scheme. Ex. 1013 at ¶ E104-107, E112-113. For example, the person would have appreciated the Hartrick security and royalty tags could be used to specify the "restrictions on usage" that are stored in the "Usage" field of the decryption ticket in the Rosen scheme with no change in the function of either system. *Id.*; Ex. 1020 at 6:12-13; Ex. 1021 at 3:53-58, 10:1-14; Ex. 1013 at ¶ E105-106, E124-127. This combination would yield obvious and predictable benefits to the Rosen scheme by increasing the granularity of control that merchants can exercise over electronic objects they sell. Ex. 1013 at ¶ E105-106. Integrating the Hartrick techniques into an implementation of the Rosen system would have been a routine engineering task for a person of ordinary skill. Ex. 1013 at ¶ E107, E113.

First, a person of ordinary skill would have found it logical to store security and royalty markup statements in the "Usage" field because would have been seen as an obvious way to specify "restrictions on usage of the electronic object" within the Rosen scheme. Ex. 1013 at ¶ E108, E124; Ex. 1020 at 6:12-13. That person consequently could have modified the MTA to include the specialized SGML tags specifying the different manners of use for the electronic object when creating each decryption ticket. Ex. 1013 at ¶ E108-112, E125-127; *see* Ex. 1021 at 3:53-58, 10:1-14. For example, the MTA could use a "Do Not Copy" tag (which prevents a

user from copying, printing, or transmitting) to specify that a user could only electronically display an electronic object, or a "Do Not Distribute" tag to specify that a user could both display and print the electronic object. Ex. 1013 at ¶ E109, E128; *see* § IV.B.2; Ex. 1021 at 3:28-32, 3:48-4:9. The MTA also could use different types of royalty tags to specify additional rights a user could exercise for a fee, such a "print-royalty" tag specifying a fee for printing (*e.g.*, a nominal fee since the user already purchased the electronic version), and a "copy-royalty" tag specifying a different fee for making a copy (*e.g.*, full price). *See* § IV.B.2; Ex. 1021 at 3:28-32, 6:9-22, 9:11-23; Ex. 1013 at ¶ E97-98, E110-111. A person of skill would have recognized that SGML was a convenient mechanism for specifying usage information because it is highly configurable and it is simple to change the dictionary of tags available for use in any particular system. Ex. 1013 at ¶ E86, E97-98, E72.

When integrating the systems, a person of ordinary skill would have considered it an obvious implementation choice to have the security tags to grant affirmative rights—*e.g.*, a "Display" tag (instead of "Do Not Copy"), or a "Print" tag and "Display" tag (instead of "Do Not Distribute"). Ex. 1013 at ¶ E111, E126, E92-98. Such a person of skill would have known that system security is improved when a user has no rights unless explicitly granted, as opposed to having all rights unless specifically restricted. Ex. 1013 at ¶ E126, E85-86, E111. This could be

done within the Hartrick scheme by having separate "Display" and "Print" tags, or by using a royalty tag with no fee (*e.g.*, "[display-royalty] $0.00 [/display-royalty]". Ex. 1013 at ¶ E111 E126-127. Choosing which tags to use would be a design choice that would routinely be made by that person of ordinary skill. Ex. 1013 at ¶ E86, E97, E71.

Also, while Hartrick describes use of SGML tagging technique in the context of softcopy books, a person of ordinary skill would recognize it could be applied to any type of electronic object, including one distributed via Rosen's system; the person would simply modify the tags accordingly to reflect the actions associated with other types of content. Ex. 1013 at ¶ E114, A118; *see* Ex. 1021 at 9:29-31 ("elements can also include graphics as well as text").

Second, a person of ordinary skill would have found it obvious to integrate Hartrick's royalty billing functionality into Rosen's MTA to allow merchants to authorize additional rights (*e.g.*, printing requests) and collect additional royalties for those operations. Ex. 1013 at ¶ E115-116; Ex. 1021 at 6:9-22, 10:7-18. The MTAs already sell various types of tickets to customers and thus have analogous functionality. Ex. 1013 at ¶ E115-116; *see* § IV.A.5; Ex. 1020 at 17:41-24:63. This modification would have obvious and predictable benefits by allowing merchants to sell additional rights to the same content. Ex. 1013 at ¶ E115-116.

Third, to enforce the security and royalty markup tags, a person of ordinary

skill would have integrated the rights checking functionality of Hartrick's royalty payment program into the CTA's protocols. Ex 1013 at ¶ E117-118, E135, E142; *see* Ex. 1021 at 6:9-22. 15:26-33. It would have been obvious to integrate this functionality into the CTA because it can be trusted to enforce security protocols. Ex. 1013 at ¶ E118, E138-142; Ex. 1020 at 4:27-32. In such a configuration, whenever a transaction application tries to render, copy, print, or transmit an electronic object, the CTA would intercept the request, check the statements in the "Usage" field, and permits access to the decryption ticket only if authorized. Ex. 1013 at ¶ E99-100, E118, E142; *see* Ex. 1021 at 6:9-22. If the operation is not authorized, the CTA would either deny the request or initiate a connection with the MTA to pay the royalty and obtain authorization. Ex. 1013 at ¶ E118, E142; *see* § IV.B.3; Ex. 1021 at 3:53-4:9, 15:34-40.

A person of skill also would have recognized that integrating the Hatrick royalty payment program into the MTA's protocols would be advantageous because it would allow authors to specify enforceable usage restrictions when providing content to a merchant. Ex. 1013 at ¶ E119, E133. Specifically, Rosen teaches that merchants store content in cleartext form and a MTA will encrypt the content and generate decryption tickets on-the-fly in response to user requests. *See* § IV.A.2-3, A.5; Ex. 1020 at 9:60-61, 24:52-55, 19:8-8; Ex. 1013 at ¶ E57, E120. Hartrick explains the author specifies usage limitations (*e.g.*, royalty fees) when

depositing a book with the publisher. *See* Ex. 1021 at 9:11-14, 5:42-45; Ex. 1013 at ¶ E120. It would have been obvious to implement the Rosen scheme by having authors specify usage limitations and royalty fees when they deposit content with the merchant as taught by Hartrick, and then having the MTA encrypt the content and generate a decryption ticket containing those limitations and fees (as tags described in Hartrick). Ex. 1013 at ¶ E120-121, E133. A person of ordinary skill would have recognized it would be beneficial to store content in encrypted for, and to give authors the ability to specify enforceable fees or restrictions on sale of content. *Id.* at ¶ E121, E133-134.

Finally, a person of skill would have adjusted Rosen's cryptographic protocols to accommodate any particular implementation that was desired. Ex. 1013 at ¶ E122. Rosen teaches communications between trusted agents should be initiated through a certificate exchange process, Ex. 1020 at 4:4-39, and a person of skill would understand any conventional way of achieving the functional objective of secure communication also could be used. Ex. 1013 at ¶ E123, E139. For example, Rosen shows that, during a purchase transaction, the CTA will initiate the Establish Session protocol by sending the MTA its digital certificate. Ex. 1020 at 17:61-67. It would be an inconsequential variation of this process to instead configure the purchase protocol such that the MTA initiated the Establish Session protocol by sending the CTA its digital certificate. Ex. 1013 at ¶ E123.

Moreover, Rosen describes one of several standard variations of the certificate exchange process; any of these processes could be integrated into Rosen without any change in function. *Id.*

D. Rosen in View of Hartrick Suggests a System Using "Usage Rights," "Trusted" "Repositories" and "Digital Documents"

1. Rosen in View of Hartrick Suggests Schemes Using "Usage Rights" Attached to Content

A person of ordinary skill would have considered it obvious to use the Hartrick security and royalty markup tags to specify the "restrictions on usage" stored in the decryption tickets within the Rosen scheme. Ex. 1013 at ¶ E104-105, E124-128, E108.

First, a person of ordinary skill would have recognized the "Usage" field of the Rosen decryption ticket stores data specifying a manner of using content. *Id.*; *see* § IV.A.2, C; Ex. 1020 at 6:12-13. That person would have recognized that Hartrick's specialized SGML tags could be implemented in the Rosen scheme by storing its tags in this "Usage" field. *See* § IV.C; Ex. 1013 at ¶ E108, E105, E124. The Hartrick tags specify different types of permissible actions (*e.g.*, a "Do Not Copy" tag grants the user the right to display and a "Do Not Distribute" tag grants the right to display and print). *See* § IV.B.2; Ex. 1021 at 3:28-32, 3:48-4:9; Ex. 1013 at ¶ E125. These rights could be implemented using separate "Display" or "Print" tags or through zero-fee royalty tags (*e.g.*, a "display-royalty" tag or a

"transmit-royalty" tag specifying a zero-dollar fee. *See* § IV.C; Ex. 1013 at ¶ E111, E126-127. Implemented in this manner, the trusted agents would use the tags to determine if a user can copy, print, store, or transmit an electronic object. *See id.* at ¶ E121; § IV.B.2; Ex. 1021 at 5:19-37, 10:5-18; Ex. 1003 at 19:15-20:28 (Possible rights include "play," "print," "copy," and "transfer"). When implemented in this manner, the "Usage" field would contains data indicating ***specific actions*** ("*manners of using or distributing*") that cam be taken with the content.

Second, a person of skill would have recognized the "Usage" field of the Rosen decryption ticket stores data specifying restrictions on a manner of use. Ex. 1013 at ¶ E124, E104. That person would also have recognized that the Hartrick royalty tags performs the same function – they specify a royalty payment amount that must be made to exercise the associated right. *See id.* at ¶ E129; § IV.B.2; Ex. 1021 at 10:1-14. Hartick shows, for example, if a user wants to print a copy of a book, an "amount" tag specifies the fee that must be paid to perform that printing action. Ex. 1021 at 12:3-12 ("The associated elements to royalty element [] are '[amount] $20.00 [/amount]' . . ."). The royalty amount set by a particular royalty tag (*e.g.*, the "display-royalty" tag) is a "*condition*" on the "*right*" of printing. Ex. 1013 at ¶ E130; *see* § IV.C. Implemented in this manner as suggested to the person of skill, the Rosen decryption ticket would contain data (a Hartrick "royalty

tag") imposing ***conditions*** on a specified manner of use. *Id.* at ¶ E130-135; Ex. 1003 at 19:4-5 ("These conditions are . . . ***fee conditions***.").

Third, the person of ordinary skill would have recognized that in the Rosen scheme, a decryption ticket (and thus the data in the "Usage" field) is permanently attached to an electronic object once purchased. *See* Ex. 1013 at ¶ E131-132; § IV.A.2; Ex. 1020 at 5:59-6:13, 4:54-55 ("A decryption ticket is always associated with a particular encrypted electronic object."). In the combined Rosen/Hartrick system, authors would specify usage restrictions and fees using the Hartrick tags when depositing content with a merchant, and the MTA, per the Rosen scheme, would generate a decryption ticket that contains that information in the "Usage" field. *See* Ex. 1013 at ¶ E133, E119; Ex. 1020 at 6:12-13; Ex. 1021 at 3:28-32, 12:7-12. Thus, "usage rights" would be permanently attached to the electronic object when the content is deposited into the system and remain with the object as it is distributed. Ex. 1013 at ¶ E132-134.

Fourth, a person of skill would have considered it an obvious implementation choice to incorporate the royalty payment program functionality linked to the specialized SGML tags of Hartrick into the trusted agents used in the Rosen scheme to enforce the markup statements in the "Usage" field. *See id.* at ¶ E115-118, § IV.B.3, C; Ex. 1021 at 6:9-22, Fig. 1; Ex. 1020 at 8:22-34. Thus, the "usage rights" are enforced by a "repository." *See* § IV.D.2.

Finally, a person of skill would have considered it to be an obvious design choice to implement the Rosen scheme by using the Hartrick technique of inserting different statements within a markup language (i.e., specialized SGML tags) to specify different rights within the "Usage" field of Rosen's decryption tickets. *See* § IV.B.2; Ex. 1021 at 10:1-7, 12:8-12; Ex. 1013 at ¶ E71, E97-98, E124, E105-108. Implemented in this manner, each right specified in the "Usage" field of the Rosen decryption ticket would be a statement in a "usage rights language." Ex. 1013 at ¶ E141, E124; *see id.* at ¶ E71-98.

Thus, Rosen in view of Hartrick suggests a combined scheme having "usage rights" permanently attached to "content" within the meaning of the claims. *Id*. at ¶ E104-135.

2. Rosen in View of Hartrick Suggests Use of Repositories

All of the challenged claims recite a "recipient computing device" or a "recipient apparatus" that is trusted and enforces usage rights. This means the recipient device or apparatus is a "repository," which is a "trusted system" that supports usage rights and "maintains physical, communications and behavioral integrity." *See* § III.D.5; Ex. 1003 at 51:34-38. The teachings of Rosen considered with those in Hartrick suggest implementing the Rosen scheme so that each transaction device is a "repository." Ex. 1013 at ¶ E136.

First, each Rosen transaction device has physically integrity. *Id.* at ¶ E137-

138, E106, E112. Each Rosen transaction device contains a trusted agent, which is a physically secure module that facilitates secure transactions between devices. *See* § IV.A1, A.3; Ex. 1020 at 4:4-39, 11:6-24. Rosen's CTD stores content in encrypted form, and the content cannot be accessed unless the CTA has the decryption ticket. *See* § IV.A.2-3, A.5; Ex. 1020 at 4:65-5:3 ("The transferred electronic object is cryptographically secure from inspection "), 4:4-39, 11:6-24; Ex. 1003 at 12:8-11 (a repository "never allow[s] non-trusted systems to access the digital works directly"), 12:22-25 ("repositories prevent access to the raw data by general devices"). Thus, each transaction device in a combined Rosen/Hartrick scheme would have physical integrity. Ex. 1013 at ¶ E138; *see* § III.D.5.

Second, each transaction device would have communications integrity. *Id.* at ¶ E139. Content is transferred between Rosen transaction devices using cryptographically secure channels. *See* § IV.A.5; Ex. 1020 at 2:13-15, 9:5-15. A trusted agent will communicate with another device only if it can provide a digital certificate proving it is a trusted agent. *See* § IV.A.4-5; Ex. 1020 at 12:22-30, 37:18-49; Ex. 1003 at 12:30-33 ("repositories will only communicate with other devices that are able to present proof that they are certified repositories"). Rosen also shows use of other conventional security features, such as encryption and nonces. *See* Ex. 1020 at 37:44-47, 15:49-51, 16:1-4; Ex. 1005 at 12:28-33 (repositories use "security measures involving encryption, exchange of digital

certificates, and nonces"). Ex. 1013 at ¶ E38-52.

Third, each transaction device would have behavioral integrity. *Id.* at ¶ E140. Rosen's decryption ticket contains a digital signature of the electronic object and the certificate of the trusted agent that created the ticket. *See* § IV.A.2, A.5; Ex. 1020 at 6:7-12, 7:30-61. When a trusted agent receives an electronic object, it validates the object against the digital signature and deletes the object if the signature is invalid. *See* § IV.A.5; Ex. 1020 at 19:13-23; *see id.* at 6:7-12. Thus, no electronic object, including software, can be installed on a transaction device unless it has a digital certificate and a valid signature authenticating its source and integrity. *Id.* at 6:7-12, 19:13-23; Ex. 1013 at ¶ E23-25. In the combined system, the Hartrick book viewing program would be distributed as a transaction application for viewing content and would be accompanied by a decryption ticket. Ex. 1013 at ¶ E106. A trusted agent would install the program only after validating the digital signature and certificate. *Id.* at ¶ E140, E24-25.

Finally, the transaction devices would support usage rights, and would do so in a combined Rosen/Hartrick system as well. The rights checking technique of the Hartrick royalty payment program is implemented in every trusted agent. *See* § IV.C; Ex. 1013 at ¶ E117-119, E142; Ex. 1021 at 6:9-22. On the customer side, this configuration would enable the CTA to enforce compliance with the data in the Usage field of the decryption ticket for purchased content. Ex. 1013 at ¶ E118,

E142. The Rosen CTA will not permit a transaction application to access the decryption ticket unless the Usage data is satisfied. *Id*. On the merchant side, this configuration would allow an author to set usage restrictions specifying how the content could be sold (*e.g.*, a minimum price) that a merchant would store as data in the "Usage" field of the decryption ticket. *Id.* at ¶ E120-121, E143; Ex. 1021 at 9:11-14. If the conditions were not met, the MTA would not generate a newly encrypted electronic object or new decryption ticket. Ex. 1013 at ¶ E143.

Thus, each transaction device in a combined Rosen/Hartrick system would be a "*repository*." *Id.* at ¶ E136-145; *see* § III.D.5.

3. Rosen and Hartrick Suggest "Digital Documents"

All of the challenged claims require a "digital document," which is a composite digital work, comprised of two or more digital works with distinct usage rights. *See* § III.E.1.

Rosen shows electronic object can be any digital content, including "electronic newspapers and books." Ex. 1020 at 4:55-57, 4:41-44. A person of skill would understand the softcopy books described in Hartrick are a type of digital content appropriate for distribution using the Rosen scheme. Ex. 1013 at ¶ E114, E22. Hartrick shows softcopy books can be distributed individually, or in a group of several books. *See* Ex. 1021 at 13:50-54. Hartrick also shows each book can contain both text and images. *Id.* at 9:29-31. Where the tags are

distributed in a separate royalty information file, each tag is associated with "coordinates" that identify appropriate book or chapter of a book that is associated with the royalty tag. *Id.* at Figs. 4 & 10, 6:23-28, 13:44-54; Ex. 1013 at ¶ E95-96, E112. When integrated in the Rosen system, a person of skill would have found it obvious to store the tags and coordinates in the "Usage" field of the decryption ticket, allowing the royalty and security tags contained in a single Right-To-Execute to be associated with different books or different chapters of a book within an electronic object. Ex. 1013 at ¶ E112, E108-114; Ex. 1020 at 6:12-13; Ex. 1021 at 3:53-58, 10:1-14. In this configuration, a softcopy book could contain multiple books, each with its own set of specialized SGML security and royalty tags. Ex. 1021 at 13:44-58, Fig. 4. Rosen in view of Hartrick teaches "*digital documents*."

E. Rosen in View of Hartrick Renders the Challenged Claims Obvious

1. Claims 1 and 18 Are Obvious

Claim 18 is representative. Claim 1 has the same preamble and the last four elements of claim 18. Claim 10 adds certain limitations discussed in § IV.E2.

a) "a method for securely rendering digital documents"

Rosen and Hartrick describe methods for distributing and rendering content. Rosen explains a customer has a CTD containing a CTA that is used to purchase and retrieve an electronic object ("*digital documents*") and a decryption ticket from a MTD. *See* § IV.A.2-3, A.5; Ex. 1020 at 4:4-39, 4:54-5:3. The Rosen CTAs and

MTAs have transaction applications for rendering content (*id.* at 8:22-34, 7:65-8:7), and, based on the guidance within Hartrick, a person of skill would have configured the CTA to enforce the "Usage" field of the decryption ticket when rendering content ("*securely rendering digital documents*"). *See* § IV.A.3, B.3, C; Ex. 1021 at 6:9-22, Fig. 1, 3:30-32, 3:53-4:9; Ex. 1013 at ¶ E117-118, E142, E20, E183-185, E187.

b) "receiving a request from a document platform to transfer a digital document . . . [and] at least one usage right" from "a document repository to the document platform . . ."

Each CTD ("*document platform*") would request and retrieve an electronic object and a decryption ticket ("*receiving a request . . . to transfer a digital document*") from a MTD ("*document repository*"). *See* § IV.A.5, B.3, C; Ex. 1020 at 4:4-39, 17:49-60; Ex. 1021 at 16:10-21, 16:26-32, 18:46-19:16; Ex. 1013 at ¶ E53-E65, E184. The decryption ticket contains a "Usage" field that in the combined system would include specialized SGML tags ("*at least one usage right*") to specify how the merchant could sell the content or how the customer could use the electronic object. *See* § IV.C; Ex. 1020 at 6:12-13; Ex. 1021 at 9:11-14, 5:42-45; Ex. 1013 at ¶ E104-114. Rosen and Hartrick thus suggest the "*receiving*" step of claim 18. Ex. 1013 at ¶ E187.

c) "authenticating the document platform by accessing at least one identifier . . . and determining whether [it] is associated with at least one [entity] authorized to use the digital document"

Rosen explains each trusted agent has a digital certificate issued by the "Trusted Agency," and the certificate contains the trusted agent's id number ("*identifier associated with the document platform or with a user*"). *See* § IV.A.4; Ex. 1020 at 10:41-12:21, 15:21-16:21, Fig. 6A; Ex. 1013 at ¶ E187, E28-37. To make a purchase in the combined system, the CTA and the MTA in a combined system would establish a session using Rosen's "Establish Session" protocol. *See* § IV.A.5; Ex. 1020 at 17:61-67; Ex. 1013 at ¶ E38-52, E219-221. In the process the CTA would send the MTA its digital certificate. Ex. 1020 at 37:29-34; *see* § IV.A.5. The MTA would validate ("*accessing*") the digital certificate and verify that the CTA's id is not on the untrusted list ("*determining whether the identifier is associated with at least one [entity] authorized to use the digital document*"). *Id.* at 37:30-42. If the certificate is valid and the CTA authorized, the process would proceed. *Id.* at 37:42-49.

> d) "if the authenticating step is successful, determining whether the digital document may be transferred and stored on the document platform based on a manner of use [] in the at least one usage right"

After establishing the session ("*the authenticating step [was] successful*"), the MTA would implement the Rosen purchase protocol and generate on the fly a new electronic object and decryption ticket for delivery to the CTA. *See* § IV.A.5; Ex. 1020 at 19:3-8; Ex. 1013 at ¶ E57, E128, E53-65. In the Rosen/Hartrick system, the MTD would securely store the content in an electronic object and a

decryption ticket that contains Usage information specified by the author when depositing content. *See* § IV.C; Ex. 1020 at 6:12-13; Ex. 1021 at 3:53-58, 10:1-14; Ex. 1013 at ¶ E118-121. Before allowing a new electronic object and decryption ticket to be generated, the MTA would check the purchased conditions against those specified by the author, and would allow the new electronic object to be generated and transferred to the CTA only if permitted ("*determining whether the digital document may be transferred and stored on the document platform based on a manner of use included in the at least one usage right*"). Ex. 1013 at ¶ E115-121; Ex. 1021 at 6:9-22; *see* § IV.C. Thus, the Rosen in view of Hartrick, teaches the "*determining*" step of claim 18. Ex. 1013 at ¶ E185-187.

> e) "if the at least one usage right allows the digital document to be transferred to the document platform, transferring the digital document and the at least one usage right . . ."

After the Rosen MTA performs "*authenticating*" and "*determining*" steps (based on determining whether the CTA has a valid digital certificate and whether the "Usage" field permits the requested sale), the MTA next would create the electronic object for delivery and generate a decryption ticket for the CTA. *See id.* at ¶ E57; § IV.A.5, C; Ex. 1020 at 19:3-8. The MTA would encrypt the content in a new key, and then create a decryption ticket containing the key and the purchased "Usage" rights. *See* § IV.A.5; Ex. 1020 at 19:3-8; Ex. 1013 at ¶ E57. The newly created object and its decryption ticket are transferred from the MTA to the CTA

("*transferring the digital document and the at least one usage right*"). Ex. 1020 at 17:49-60, 18:66-19:14, 23:13-22; Ex. 1013 at ¶ E57, E185-E187.

Claim 1 specifies the document platform "*retriev[es] . . . a digital document and at least one usage right . . . from a document repository*." In the combined Rosen/Hartrick system, the electronic object transferred from the MTA to the CTA would contain the content requested by the customer (*see* § IV.E.1.b), and therefore that combined system would perform the "*retrieving*" step involving the digital document. Ex. 1013 at ¶ E57, E185. Claim 1 also specifies the usage right contains "*a manner of use indicating the manner in which the digital document can be rendered*." In the combined Rosen/Hartrick system, the "Usage" field would contain specialized SGML tags, as suggested by Hartrick. *See* § IV.C; Ex. 1020 at 6:12-13; Ex. 1021 at 3:53-58, 10:1-14 Ex. 1013 at ¶ E104-E114, E124-E135. Such tags could include a "Do Not Copy" tag, a "Do Not Distribute" tag, a "Display," a "Print" tag, "print-royalty" tag, or a "transmit-royalty" tag, as suggested by Hartrick ("*a manner of [rendering]*"). *See* § IV.B.2, C, D.1; Ex. 1021 at 3:28-32, 3:48-4:9, 5:23-38, 6:9-22, 9:11-23; Ex. 1013 at ¶ E125-130, E108-114. Rosen in view of Hartrick suggests the "*retrieving*" step of claim 1. Ex. 1013 at ¶ E185.

f) "storing the digital document and the at least one usage right [in separate files] in the document platform"

Rosen shows the electronic object (containing content) can be stored in any memory on the CTD or MTD because the content is encrypted. Ex. 1020 at 19:8-

12. In a combined system, the usage rights would be stored in the "Usage" field of the decryption ticket, and, as Rosen shows, the decryption ticket would be stored in the CTA. *Id.* at 6:12-13, 9:60-61, 23:17-21; Ex. 1013 at ¶ E138-E141. Thus, the electronic object and the decryption ticket would be separate files. *Id.* at 4:41-44, 4:54-5:3, 6:3-4; Ex. 1013 at ¶ E184-185, E112. Rosen teaches the "*storing*" step of claims 1 and 18. Ex. 1013 at ¶ E185-187.

g) "determining . . . whether the digital document may be rendered based on the at least one usage right"

A person of skill would have considered it obvious based on Hartrick to configure the Rosen CTAs and MTAs to perform Hartrick's royalty payment program, *i.e.* intercept any requests to copy, store, print, or transmit an electronic object. *See* § IV.B.3; Ex. 1021 at 6:9-22; Ex. 1013 at ¶ E115-121, E99-103. When the CTA in Rosen is configured in this manner as taught by Hartrick, it would check the "Usage" field of a decryption ticket before permitting the requested operation to occur ("*determining . . . whether the digital content may be rendered*"). *See* § IV.B.3, C; Ex. 1021 at 6:9-22; Ex. 1013 at ¶ E117-118. In this configuration, when a customer uses a transaction application (*e.g.*, the book viewing program in Rosen) to access the content in an electronic object, the CTA in that CTD would check the "Usage" field of the decryption ticket before allowing the transaction application to access the ticket and decrypt the content. *See* § IV.B.3, C; Ex. 1020 at 6:12-13; Ex. 1021 at 6:9-22; Ex. 1013 at ¶ E117-118,

E113. Thus, Rosen in view of Hartrick suggests the "*determining*" step of claims 1 and 18. Ex. 1013 at ¶ E185-187.

h) "if . . . render[ing] on the document platform [is allowed], rendering the digital document"

If, when a transaction application on the CTA would check the "Usage" field of the decryption ticket, the CTA would determine the request is permitted (*e.g.*, display, print, or transmit), the CTA would allow the transaction application access to the decryption ticket; otherwise the request is denied ("*rendering* . . ."). *See* § IV.B.3, C, IV.E.1.g; Ex. 1021 at 5:19-38; 21:56-22:3, 22:7-10 (print); 22:34-38, 22:42-45 (copy); 23:13-14, 23:21-24 (transmit); Ex. 1013 at ¶ E118. Rosen in view of Hartrick suggests the "*rendering*" step of claims 1 and 18. Ex. 1013 at ¶ E185-187.

2. Claim 10 Is Obvious

Claim 10 recites the same elements as claim 18, but adds several limitations:

a) storing a digital document and at least one usage right in separate files in a document repository . . ."

In a Rosen/Hartrick system, the merchant would be configured to securely store the content in an electronic object and would create and store a decryption ticket that contains "Usage" information specified by the author when the content was deposited. *See* § IV.C; Ex. 1021 at 9:11-14; Ex. 1013 at ¶ E108, E121, E104-121. The decryption ticket containing the "Usage" information would be a separate file from the electronic object. Ex. 1020 at 4:41-44, 4:54-5:3, 6:3-4; Ex. 1013 at

¶ E184, E112, E186.

b) "receiving a request from a document platform for access to the digital document"

Rosen and Hartrick teach receiving a request to "transfer" a digital document. *See* § IV.E.1.b. A request to transfer is a type of request for access. Ex. 1013 at ¶ E186.

c) "determining, by the document platform, whether the request may be granted . . ."

In Claim 10, "*the determining step includ[es] authenticating the document platform and determining whether the at least one usage right includes a manner of use that allows transfer of the digital document to the document platform*."

The Rosen MTDs "*authenticate*" a CTD ("*document platform*") and they "*determine*" whether a request to transfer can be granted. *See* § IV.E.1.c-d; Ex. 1020 at 37:42-49; Ex. 1021 at 6:9-22. A person of skill also would consider implementing the "*determining*" step on the CTDs to have been an obvious implementation choice. Ex. 1013 at ¶ E186, E58. For example, Rosen shows that when a CTA receives an electronic object and a decryption ticket, the CTA will validate the object's integrity and ensure it is the requested object. Ex. 1020 at 19:17-39. A person of skill would have considered it to be obvious and logical to also validate the "Usage" field during this process to ensure that the correct rights were received and the received rights would permit the customer to render the

content in the object. Ex. 1013 at ¶ E186, E58. It would have been obvious, based on guidance within Rosen, to implement the Rosen/Hartrick system by having the CTA in the CTD ("*document platform*") determine whether a request can be granted. *Id.*

> d) "transferring the digital document and the at least one usage right. . . ", "storing the digital document and the at least one usage right. . . in [] separate file[s]", and "rendering . . ."

Each of these steps are analogous to those in claims 1 and 18, and as described with regard to claim 18, the combined Rosen/Hartrick system would perform each step. *See* § IV.E.1.e (the "*transferring*" step); § IV.E.1.f (the "*storing*" step); § IV.E.1.h,(the "*rendering*" step); Ex. 1013 at ¶ E185-187.

3. Claims 8, 16, and 24 Are Obvious

As explained in § IV.A.3 and E.1.f, the electronic object is encrypted and can be stored in any memory, and the decryption ticket is separate file that is stored in the trusted agent. Ex. 1020 at 4:41-45, 9:60-61, 23:17-21. Both files are stored on the same transaction device. *Id.*; *see also id.* at 24:52-55. Rosen in view of Hartrick renders obvious claims 8, 16, and 24. Ex. 1013 at ¶ E189-191.

F. No Secondary Considerations Exist

Rosen in view of Hartrick teaches systems and processes that render *prima facie* obvious each of the challenged claims of the '072 patent. No secondary indicia of non-obviousness exist having a nexus to the putative "invention" of the

’072 patent contrary to that conclusion. Petitioner reserves its right to respond to any assertion of secondary indicia of non-obviousness advanced by Patent Owner.

V. Conclusion

For the foregoing reasons, Petitioner respectfully submits that the evidence presented in this petition establishes a reasonable likelihood that Petitioner will prevail in establishing claims 1, 8, 10, 16, 18, and 24 of the ’072 patent are unpatentable, and requests that Trial be instituted to cancel these claims.

Dated: December 22, 2014

Respectfully Submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Registration No. 43,401
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005
jkushan@sidley.com
(202) 736-8914
Attorney for Petitioner

PETITION FOR *INTER PARTES* REVIEW

OF U.S. PATENT NO. 7,523,072

Attachment A:

Proof of Service of Petition

CERTIFICATE OF SERVICE

I hereby certify that on this 22nd day of December, 2014, a copy of this Petition for *Inter Partes* Review, Attachments and Exhibits, has been served in its entirety by Federal Express on the following address for Patent Owner:

ContentGuard Holdings, Inc.
6900 N. Dallas Parkway, Suite 850
Plano, Texas, 75024

Prosecution Counsel:

Marc S. Kaufman
Reed Smith LLP
1301 K Street, N.W.
Suite 1100 – East Tower
Washington, DC 20005

Litigation Counsel:

Samuel F. Baxter (sbaxter@mckoolsmith.com)
MCKOOL SMITH, P.C.
104 East Houston, Suite 300
Marshall, Texas 75670

Respectfully submitted,

/Jeffrey P. Kushan/
Jeffrey P. Kushan
Reg. No. 43,401
Attorney for Petitioner

PETITION FOR *INTER PARTES* REVIEW

OF U.S. PATENT NO. 7,523,072

Attachment B:

Exhibit List

Exhibit #	Reference Name
1001	U.S. Patent No. 6,963,859
1002	File History of U.S. Patent No. 6,963,859
1003	U.S. Patent No. 7,523,072
1004	File History of U.S. Patent No. 7,523,072
1005	U.S. Patent No. 8,370,956
1006	File History of U.S. Patent No. 8,370,956
1007	U.S. Patent No. 8,393,007
1008	File History of U.S. Patent No. 8,393,007
1009	U.S. Patent No. 7,269,576
1010	File History of U.S. Patent No. 7,269,576
1011	U.S. Patent No. 7,225,160
1012	File History of U.S. Patent No. 7,225,160
1013	Declaration of Alan Sherman, Ph. D. regarding patents 859, 072, 956, 007, 576
1014	Curriculum Vitae for Alan Sherman
1015	[RESERVED]
1016	S. White & L. Comerford, ABYSS: A Trusted Architecture for Software Protection (1987)
1017	D. Denning, Cryptography and Data Security (1982)
1018	U.S. Patent No. 6,135,646 to Kahn
1019	Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project (Jan. 1, 1994)
1020	U.S. Patent No. 5,557,518 to Rosen
1021	EP 0567800 A1 to Hartrick
1022	File History for U.S. Patent No. 6, 135,646 to Kahn

Exhibit #	Reference Name
1023	U.S. Patent No. 5,629,980 to Stefik
1024	5,477,263 (O'Calleghan)
1025	U.S. Patent No. 5,260,999, issued November 9, 1993 to Wyman
1026	J. Moffett et al., SPECIFYING DISCRETIONARY ACCESS CONTROL POLICY FOR DISTRIBUTED SYSTEMS, Computer Communications, vol 13 no 9, pp 571-580 (Nov. 1990)
1027	R. Mori & M. Kawahara, Superdistribution: The Concept and Architecture, The Transactions of The IEICE, Vol. E73, No. 7, pp. 1133-1146 (July 1990)
1028	European Patent Publication 0 268 139
1029	U.S. Patent No. 5,412,717 to Fischer
1030	The Copy-Protection Wars, PC Magazine
1031	US 4,658,093 to Hellman
1032	US 5,940,504 to Griswold
1033	G. Davida et al., Defending Systems Against Viruses through Cryptographic Authentication, IEEE 1989
1034	V. Cina et al., ABYSS: A Basic Yorktown Security System: PC Asset Protection Concepts, IBM Research Report Number RC 12401 (Dec. 1986)
1035	U.S. 5,109,413 to Comerford
1036	S. Weingart, Physical Security for the μABYSS System, Proceedings of the IEEE Symposium on Security and Privacy (Apr. 27-29, 1987)
1037	FIPS 140-1
1038	4,278,837 to Best
1039	William Aspray, The Stored Program Concept, IEEE Spectrum Sept. 1990
1040	Glenn C. Reid, Thinking in Postscript, Addison-Wesley (1990)
1041	Bruce Schneier, Applied Cryptography (Chapters 1-3, 7, 12, 13, 17) (1994)
1042	Samuelson, Intellectual Property Rights for Digital Library and Hypertext Publishing Systems: An Analysis of Xanadu (Dec. 1991)
1043	Kahn & Cerf, "The Digital Library Project Volume 1: The World of Knowbots (Draft)" (1988)

Exhibit #	Reference Name
1044	Internet Dreams - Stefik foreword
1045	CNRI Digital Library Workshop
1046	Diffie-Hellman, New Directions in Crypto 1976
1047	X.509 Standard
1048	RFC 1422, Privacy Enhanced Mail (PEM)
1049	Steiner et al., Kerberos: An Authentication Service for Open Network Systems (MIT 1988)
1050	Needham & Schroeder, Using Encryption for Authentication in Large Networks of Computers (Dec. 1978)
1051	J. Saltzer & M. Schroeder, The Protection of Information in Computer Systems, Proceedings of the IEEE, Vol. 63, No. 9 (Sept. 1975)
1052	ContentGuard's Opening Claim Construction Brief, 2:13-cv-01112 (EDTX) Dkt No. 304
1053	U.S. Patent Application File History No. 09/778,001
1054	U.S. Patent Application File History Nos. 08/967,084 and 08/344,760
1055	U.S. Patent No. 4,977,594 to Shear
1056	Henry H. Perritt, Jr., "*Knowbots, Permissions Headers and Contract,*" Paper for the Conference on Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment (April 30, 1993)
1057	*Dyad: A System for Using Physically Secure Coprocessors*, J.D. Tygar and Bennett Lee, Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project (Jan. 1, 1994)
1058	"*Copyright and Information Services in the Context of the National Research and Education Network*," R.J. Linn, Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project (Jan. 1, 1994)
1059	"*The Strategic Environment for Protecting Multimedia*," Brian Kahin, Proceedings of the Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment, Journal of the Interactive Multimedia Association Intellectual Property Project (Jan. 1, 1994)

Exhibit #	Reference Name
1060	Amir Herzberg, Shlomit S. Pinter, "Public Protection of Software," in Advances in Cryptology: Proc. Crypto 85, Hugh C. Williams (cd.), pp. 158 (1986)
1061	S. White & L. Comerford, ABYSS: A Trusted Architecture for Software Protection (1990)
1062	T. Berners-Lee & D. Connolly, RFC 1866, Hypertext Markup Language v2.0 (Nov. 1995)
1063	[RESERVED]
1064	[RESERVED]
1065	[RESERVED]
1066	[RESERVED]
1067	[RESERVED]
1068	Summons in Case No. 2:13-CV-01112
1069	Declaration of Dr. Goodrich in support of ContentGuard's Opening Claim Construction Brief – Exhibit K of Doc. No. 304