Trials@uspto.gov
571-272-7822

Paper 57
Entered: June 26, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZTE CORPORATION AND ZTE (USA) INC.,
Petitioner,

v.

CONTENTGUARD HOLDINGS, INC.,
Patent Owner.

Case IPR2013-00139
Patent 7,269,576 B2

Before JAMESON LEE, MICHAEL W. KIM, and MICHAEL R. ZECHER, *Administrative Patent Judges*.

LEE, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. BACKGROUND

A. Introduction

On February 12, 2013, Petitioner ("ZTE") filed a Petition for *inter partes* review of claims 1-36 of U.S. Patent No. 7,269,576 B2 ("the '576 patent"). Paper 2. Petitioner filed a Revised Petition ("Pet.") on February 15, 2013.[1] Paper 9. On July 9, 2013, the Board instituted trial for claims 18-21, 25-28, and 31-36, under 35 U.S.C. § 102(b), as anticipated by European Patent Publication 0 268 139 ("EP '139"). Paper 15 ("Dec.").

After institution of trial, Patent Owner ("ContentGuard")[2] filed a Patent Owner Response (Paper 33, "PO Resp."), and did not file a Motion to Amend Claims. ZTE subsequently filed a Reply. Paper 39 ("Reply").

A consolidated oral hearing for IPR2013-00133, IPR2013-00137, IPR2013-00138, and IPR2013-00139, each involving the same Petitioner and Patent Owner, was held on February 26 and 27, 2014. The transcript of the consolidated hearing has been entered into the record. Papers 54-56.

We have jurisdiction under 35 U.S.C. § 6(c). This final written decision is issued pursuant to 35 U.S.C. § 318(a).

---

[1] Hereinafter, all use of the term "the Petition" in this decision refers to the Revised Petition unless indicated otherwise.

[2] The mandatory notices filed pursuant to 37 C.F.R. § 42.8(b)(1) indicate that ContentGuard Holdings, Inc. and Pendrell Corporation are real parties-in-interest. Paper 11, 2.

Claims 18-21, 25-28, and 31-36 of the ’576 Patent have not been proved unpatentable.

B. Related Proceedings

ZTE indicates that the ’576 patent is involved in co-pending litigation titled *ContentGuard Holdings Inc. v. ZTE Corp. et al.*, No. 3:12-cv-01226 (S.D. Cal.). Pet. 1. ZTE also filed five other petitions seeking *inter partes* review of the following patents of ContentGuard: U.S. Patent No. 7,523,072 (IPR2013-00133); U.S. Patent No. 7,225,160 (IPR2013-00134); U.S. Patent No. 7,359,884 (IPR2013-00136); U.S. Patent No. 6,963,859 (IPR2013-00137); and U.S. Patent No. 7,139,736 (IPR2013-00138). *Id*.

C. The ’576 Patent

The subject matter of the ’576 patent relates to the distribution of digitally encoded works and the enforcement of usage rights. Ex. 1001, 1:5-6. According to the ’576 patent, an issue facing the publishing and information industries is how to prevent the unauthorized and unaccounted distribution or usage of electronically published materials. *Id*. at 1:10-13. In particular, a major concern, according to the ’576 patent, is the ease with which electronically published works can be “perfectly” reproduced and distributed. *Id*. at 1:24-25. According to the ’576 patent, one way to curb unaccounted distribution is to prevent unauthorized copying and transmission. *Id*. at 1:44-46. Another way, according to the ’576 patent, is to distribute software which requires a “key” to enable its use. *Id*. at 1:60-61. The ’576 patent discloses that, although such distribution and protection schemes prevent unauthorized distributions, they do so by sacrificing the

potential for subsequent revenue bearing uses. *Id*. at 2:56-60. For example, the '576 patent discloses that it may be desirable to allow the lending of a purchased work to permit exposure of the work to potential buyers, permit the creation of a derivative work for a fee, or permit copying the work for a fee. *Id*. at 2:60-65. The '576 patent discloses that it solves these problems by both permanently attaching usage rights to digital works, and by placing elements in repositories, which store and control the digital works and enforce the usage rights associated therewith. *Id*. at 3:53-4:15.

Figure 1 of the '576 patent is reproduced below:

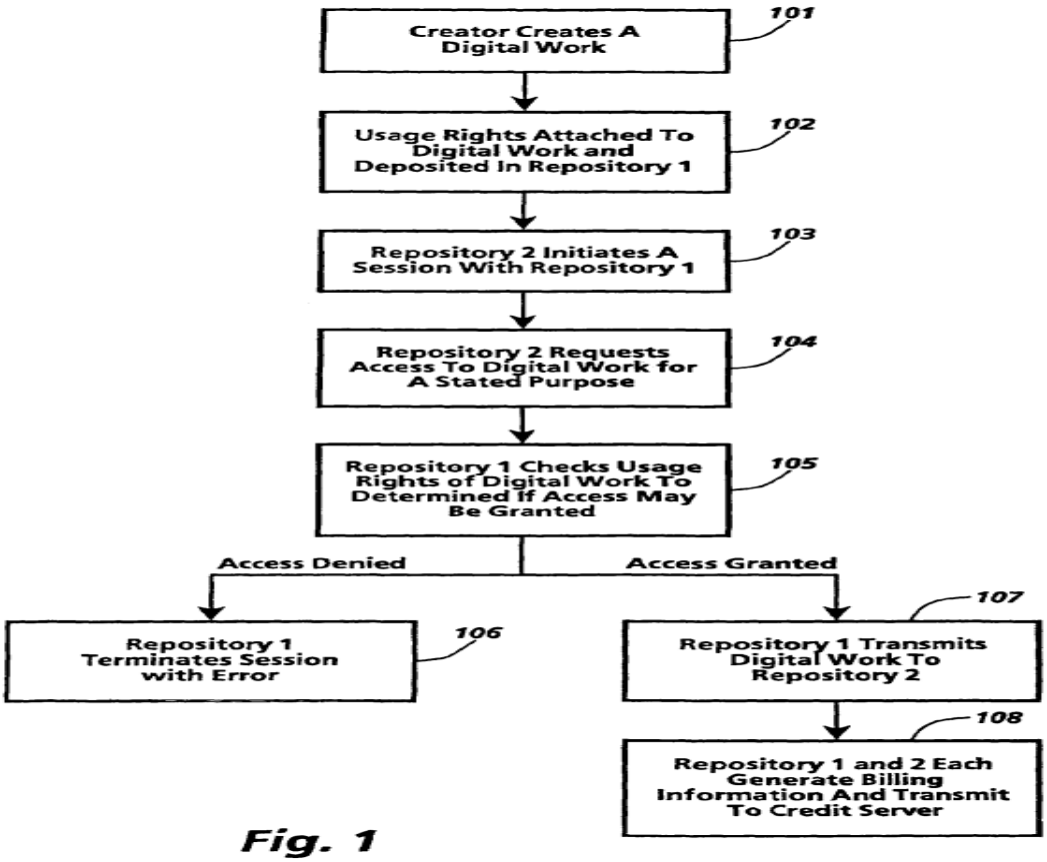

Figure 1 illustrates the basic operations of the disclosed invention.

According to the embodiment of Figure 1, at step 101, a creator creates a digital work. Ex. 1001, 7:1-2. At step 102, the creator determines the appropriate usage rights and fees, attaches them to the digital work, and stores the digital work with the associated usage rights and fees in repository 1. *Id*. at 7:2-7. At step 103, repository 1 receives a request to access the digital work from repository 2. *Id*. at 7:7-9. Such a request, or session initiation, includes steps that help ensure that repository 1 and repository 2 are trustworthy. *Id*. at 7:7-12. At step 104, repository 2 requests access to the digital work stored in repository 1 for a stated purpose, *e.g.*, to print the digital work or obtain a copy of the digital work. *Id*. at 7:13-17. At step 105, repository 1 checks the usages rights associated with the digital work stored therein to determine if access to the digital work may be granted. *Id*. at 7:17-24. At step 106, if access is denied, repository 1 terminates the session with repository 2 by transmitting an error message. *Id*. at 7:24-25. At step 107, if access is granted, repository 1 transmits the digital work to repository 2. *Id*. at 7:25-27. At step 108, both repository 1 and 2 generate billing information prior to transmitting the billing information to a credit server. *Id*. at 7:27-30. The use of both repositories 1 and 2 for billing prevents attempts to circumvent the billing process. *Id*. at 7:30-31.

One embodiment described in the ’576 patent relates to enforcing usage rights in rendering systems. Ex. 1001, 8:16-67. Rendering systems are systems that can render a digital work into its desired form, such as by printing a file on a printer or executing a software program in a processor.

Id. at 8:19-22, 8:37-38, 8:53-55. Other examples of rendering systems include display, video, or audio systems. *Id*. at 51:65-67. Rendering systems include repositories that store digital works and maintain the security features of the '576 patent. *Id*. at 8:22-23, 12:25-34. Repositories in rendering systems can request to perform various usage transactions, such as play or print transactions, that obtain a digital work from a remote repository and then provide it to an attached rendering device to be rendered. *Id*. at 30:23-35, 36:18-37:26.

Figure 4a of the '576 patent is reproduced below:

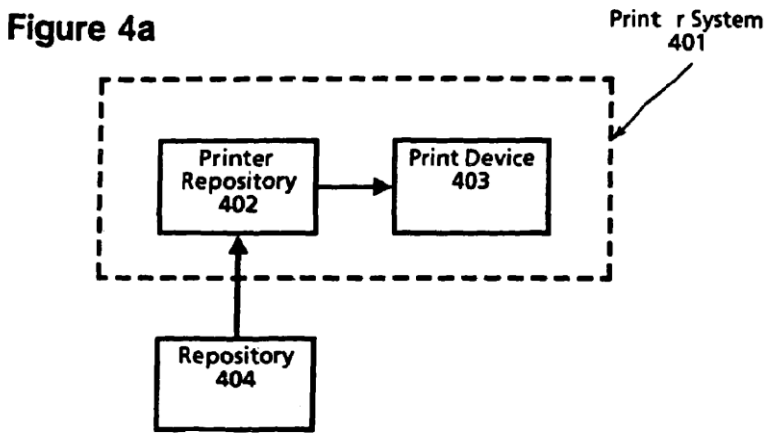

Figure 4a illustrates an example of a rendering system

According to the embodiment of Figure 4a, printer system (401), including print device (403) and printer repository (402), is attached to external repository (404) that contains digital works. Ex. 1001, 8:26-29, 48-51. The printer repository can obtain a copy of the digital work to be provided to the rendering device. *Id*. at 8:36-38. That is accomplished by

invoking a specific type of usage transaction called a print transaction. *Id*. at 36:55-37:26. A print transaction begins with a requestor repository sending a message requesting permission to obtain and print a specified digital work that is stored in a server repository. *Id*. at 36:55-37:26. Certain rendering transactions require the presence of a digital ticket or an authorization object in a repository requesting a digital work before the digital work can be provided. *Id*. at 36:45-46, 37:18-19, 31:6-9. Repositories acquire digital tickets through authorization transactions that request authorization objects from a remote authorization repository. *Id*. at 41:31-42:16. If the repository requesting the digital work is in possession of an authorization object, the server repository determines whether the requestor is permitted to perform the transaction based on usage rights related to the digital work. *Id*. at 36:45-46, 37:18-19, 30:59-31:49. Once the transaction is determined as being permitted, the digital work is transmitted to the repository requesting the digital work, and then the digital work is rendered. *Id*. at 36:47-50, 37:20-22.

D. Illustrative Claim

Claim 18 is an independent claim from which claims 19-21, 25-28, and 31-36 directly or indirectly depend, and is reproduced below:

> 18. A method for controlling rendering of digital content on an apparatus having a rendering engine configured to render digital content and a storage for storing the digital content, said method comprising:

> specifying rights within said apparatus for digital content stored in said storage, said rights specifying how digital content can be rendered;
>
> storing digital content in said storage;
>
> receiving a request for rendering of said digital content stored in the storage;
>
> checking whether said request is for a permitted rendering of said digital content in accordance with said rights specified within said apparatus;
>
> processing the request to make said digital content available to the rendering engine for rendering when said request is for a permitted rendering of said digital content;
>
> authorizing a *repository* for making the digital content available for rendering, wherein the digital content can be made available for rendering only by an authorized repository, the repository performing the steps of:
>
> making a request for an authorization object required [sic] to be included within the repository for rendering of the digital content; and
>
> receiving the authorization object when it is determined that the request should be granted.

Ex. 1001, 53:57-54:16 (emphasis added).

II. ANALYSIS

The only ground instituted for trial is that of the alleged anticipation, under 35 U.S.C. § 102(b), of claims 18-21, 25-28, and 31-36 by EP ’139

(Ex. 1012). ZTE has to prove unpatentability by a preponderance of the evidence. 35 U.S.C. § 316(e). In patent law, "the name of the game is the claim." *In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998). Therefore, we begin with claim construction, and then follow with specific analysis of the prior art.

A. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are interpreted according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012). The terms also are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). If an inventor acts as his or her own lexicographer, the definition must be set forth in the specification with reasonable clarity, deliberateness, and precision. *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1249 (Fed. Cir. 1998).

An extraneous limitation should not be read into the claims from the specification. *E.g., E.I. du Pont de Nemours & Co. v. Phillips Petroleum Co.*, 849 F.2d 1430, 1433 (Fed. Cir. 1988). An extraneous limitation is one the presence of which in a claim is unnecessary to make sense of the claim. *See, e.g., In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994); *Renishaw PLC*, 158 F.3d at 1249. The construction that stays true to the claim language and most naturally aligns with the inventor's description is likely

the correct interpretation. *See Renishaw PLC*, 158 F.3d at 1250. The challenge is to interpret claims without unnecessarily importing limitations from the specification into the claims. *See E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003).

repository

In its petition, ZTE does not provide an explicit construction for "repository." In the Patent Owner Preliminary Response, ContentGuard contended that "repository" should be interpreted as "a trusted system for supporting usage rights." Prel. Resp. 21. When instituting trial, we construed "repository" as "a trusted system which maintains physical, communications and behavioral integrity, and supports usage rights." Dec. 12. For reasons discussed below, we adhere to the same interpretation.

The specification provides a glossary which recites the following meaning for "repository":

> Conceptually a set of functional specifications defining core functionality in the support of usage rights. *A repository is a trusted system in that it maintains physical, communications and behavioral integrity*.

Ex. 1001, 52:1-6 (emphasis added). By setting forth the term in a glossary and using the verb "is" following "repository" in the second sentence, the specification sets forth an explicit definition of "repository" as "a trusted system in that it maintains physical, communications and behavioral integrity." The first sentence is also relevant to the definition of "repository" because it specifies that the repository supports usage rights. Accordingly,

we construe "repository" as "a trusted system which maintains physical, communications and behavioral integrity, and supports usage rights."

Our analysis does not end here. In order to understand "a trusted system" it is necessary to construe "physical integrity," "communications integrity," and "behavioral integrity." Those terms are described in a section of the specification labeled "[r]epositories." For "physical integrity," the specification describes:

> Physical integrity refers to the integrity of the physical devices themselves. *Physical integrity applies both to the repositories and to the protected digital works*. Thus, the higher security classes of repositories themselves may have sensors that detect when tampering is attempted on their secure cases. *In addition to protection of the repository itself, the repository design protects access to the content of digital works*. In contrast with the design of conventional magnetic and optical devices-such as floppy disks, CD-ROMs, and videotapes-*repositories never allow non-trusted systems to access the works directly*. A maker of generic computer systems cannot guarantee that their platform will not be used to make unauthorized copies. The manufacturer provides generic capabilities for reading and writing information, and the general nature of the functionality of the general computing device depends on it. Thus, a copy program can copy arbitrary data. This copying issue is not limited to general purpose computers. It also arises for the unauthorized duplication of entertainment "software" such as video and audio recordings by magnetic recorders. Again, the functionality of the recorders depends on their ability to copy and they have no means to check whether a copy is authorized. In contrast, *repositories prevent access to the raw data by general devices* and can test explicit rights and conditions before copying or otherwise granting access. *Information is only accessed by protocol between trusted repositories*.

Ex. 1001, 12:35-61 (emphases added). Much of the above description makes use of permissive terms such as "may" and "can" and, thus, do not reflect or indicate a required limitation for physical integrity. The specification also appears to use the terms or phrases in each of the following three groups interchangeably:

1. data, content, digital work, information;
2. non-trusted system, general device; and
3. "never allow access" and "prevent access."

When referring to the relationship between the repository and data, the specification uses absolute terms such as "never" and "only." In light of the foregoing, we construe "physical integrity" as "preventing access to information by a non-trusted system."

For "communications integrity," the specification describes the following:

> Communications integrity refers to the integrity of the communications channels between repositories. Roughly speaking, communications integrity means that repositories cannot be easily fooled by "telling them lies." Integrity in this case refers to the property that *repositories will only communicate with other devices that are able to present proof that they are certified repositories*, and furthermore, that the repositories monitor the communications to detect "impostors" and malicious or accidental interference. Thus *the security measures involving encryption, exchange of digital certificates, and nonces described below are all security measures aimed at reliable communication* in a world known to contain active adversaries**.**

Ex. 1001, 12:62-13:7 (emphases added). We construe "communications integrity" as "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." The Encyclopedia of Cryptography defines "nonce" as "[a] number used in a cryptographic protocol to indicate the unique character of a message." ENCYCLOPEDIA OF CRYPTOGRAPHY 197 (1997) (Ex. 3001).

For "behavioral integrity," the specification describes:

> Behavioral integrity refers to the integrity in what repositories do. What repositories do is determined by the software that they execute. The integrity of the software is generally assured only by knowledge of its source. Restated, a user will trust software purchased at a reputable computer store but not trust software obtained off a random (insecure) server on a network. *Behavioral integrity is maintained by requiring that repository software be certified and be distributed with proof of such certification, i.e. a digital certificate.* The purpose of the certificate is to authenticate that the software has been tested by an authorized organization, which attests that the software does what it is supposed to do and that it does not compromise the behavioral integrity of a repository. *If the digital certificate cannot be found in the digital work or the master repository which generated the certificate is not known to the repository receiving the software, then the software cannot be installed.*

Ex. 1001, 13:8-33 (emphases added). We construe "behavioral integrity" in the context of a repository as "requiring software to include a digital certificate in order to be installed in the repository."

The record is not without evidence in contrary to our interpretation. That is not unusual. The nature of interpretation is to come to the

appropriate conclusion in light of all of the evidence. All of the evidence does not have to point uniformly in a single direction.

For instance, the specification in Table 2 indicates ten different levels of security for repositories, and the lowest level, i.e., level "0," is described as follows:

> Open system. Document transmission is unencrypted. No digital certificate is required for identification. The security of the system depends mostly on user honesty, since only modest knowledge may be needed to circumvent the security measures. The repository has no provisions for preventing unauthorized programs from running and accessing or copying files. The system does not prevent the use of removable storage and does not encrypt stored files.

Ex. 1001, 15:30-41. Thus, according to Table 2, repositories are not all trusted systems. Level "0" security means having an open system lacking in physical, communications, and behavioral integrity, and without support for managing usage rights. That is directly contrary to the meaning of "repository" as defined in the glossary. For reasons discussed below, we adhere to the definition provided in the glossary. The contrary evidence based on level "0" security shown in Table 2 is insufficient to outweigh the rest of the evidence including, in particular, the explicit definition provided in the glossary. We make our determination based on the totality of the evidence.

As noted above, the disclosed invention is about distribution of and usage rights enforcement of digital works. The problems described in the background portion of the specification concerns unauthorized and

unaccounted distribution or usage of electronically published materials. Ex. 1001, 1:24-43. The '576 patent states that it solves preexisting problems by both permanently attaching usage rights to digital works and placing elements in repositories which enforce those usage rights. Ex. 1001, 3:53-4:15.

Here, the definition set forth in the glossary for "repository" is consistent with the description of the acknowledged prior art, and the objective or goal to be achieved by the invention of the '576 patent. The specification also contains detailed preferred embodiments utilizing repositories, which are trusted systems to provide usage control for digital works. Ex. 1001, 12:25-34, 26:20-44, 43:36-50:26.

The bulk of the disclosure consistently is directed to repositories which are trusted systems for providing usage control for digital works. For example, the specification states:

> *The enforcement elements of the present invention are embodied in repositories.* Among other things, repositories are used to store digital works, control access to digital works, bill for access to digital works and maintain the security and integrity of the system.

Ex. 1001, 6:50-54 (emphasis added). Other references to "repository" in the specification that recite necessary features of repositories also support the definition in the glossary that a repository is a trusted system:

> The core repository services 1302 comprise a set of functions *required by each and every repository*. The core repository services 1302 include the session initiation transactions which are defined in greater detail below. This set of services also includes a generic ticket agent which is used to "punch" a

> digital ticket and a generic authorization server for processing authorization specifications.

Ex. 1001, 14:45-51 (emphasis added). In another example, the specification discloses that "[a]s a prerequisite to operation, a repository will require possession of an identification certificate," and that "identification certificates 1306 are required to enable the use of the repository." Ex. 1001, 13:42-44, 14:56-57. Indeed, by using words such as "require" and "required," such examples amply support the definition provided in the glossary that a repository is a trusted system.

In summary, even applying the rule of broadest reasonable construction consistent with the specification, the weight of the evidence supports the definition provided in the glossary. We regard as significant that the definition states in an unequivocal manner that a repository "is a trusted system."

According to ContentGuard, our interpretation of "repository" is incorrect because it is too broad in one respect and too narrow in another. PO Resp. 8-11. For reasons discussed below, however, the specification of the '576 patent does not support adequately either contention. On the record before us, we are unpersuaded by ContentGuard's contentions.

We address below, in turn, first the contention that our construction is too broad, and then the contention that our construction is too narrow.

1.

ContentGuard contends that our construction regarding "behavioral integrity" as "requiring software to include a digital certificate in order to be installed in the repository" is "excessively broad" unless the software is

limited to that which makes the repository operative—software which ContentGuard believes is referred to in the specification as "repository software." *Id*. at 8. We reproduce ContentGuard's argument, in more detail, below:

> [The Board's construction] is too broad because it is not restricted to what the '576 patent refers to as "repository software"—that is software that makes the repository operative. (*See* Ex. 1001, 13:14-17.) According to the '576 patent Specification, "[b]ehavioral integrity refers to the integrity in what repositories do." (Ex. 1001, 13:8-9.) What repositories do, in turn, "is determined by the software that they execute." (*Id*., 13:9-10)
>
> But not all software relates "to the integrity in what repositories do." (*Id*., 13:8-9) Repositories, along with usage rights, are used to manage the use and distribution of digital content. (*E.g.*, Ex. 1001, 4:6-7, 6:50-54, 12:25-33, 52:1-6.) Allowing them to do so, repositories can perform several functions to implement the transmission of content and usage rights. (*E.g.*, Ex. 1001, 13:65-14:3.) But content itself does not necessarily supply that function to a repository. (Ex. 2013, Goodrich Dec., ¶ 41; *see also* ¶¶ 37-40.) Rather, repository software implements the repository functions that are used to manage the use and distribution of the content. (Ex. 1001, 13:51-56, 14:7-10, 34-43.) Thus, since "[b]ehavioral integrity refers to the integrity in what repositories do," the relevant software is not any "software . . . to be installed in the repository," but the software the repository uses to manage the use and distribution of content.

PO Resp. 8-9.

On what repositories do, ContentGuard's argument overlooks and fails to discuss the portions of the specification which indicate that

repositories themselves also can be rendering devices which run and execute the software type digital works, the usage rights of which they control. For instance, the '576 patent states the following with regard to software runnable on a repository:

> An Install transaction is a request to install a digital work as *runnable software on a repository*. In a typical case, the requester repository is a *rendering repository* and the software would be a new kind or *new version of a player*.

Ex. 1001, 42:18-21 (emphasis added). This disclosure in the specification does not support ContentGuard's contention that a repository merely manages the use and distribution of digital content, such as software, and does not perform, run, or execute that digital content. The above-quoted disclosure refers to a digital work that is "runnable software on a repository," and states that, in a typical case, the repository asking for the digital work is itself a rendering repository that identifies the software digital work not as operating software, but application software. The specification conveys much information contrary to ContentGuard's contention. ContentGuard does not explain such disclosure and does not point to any testimony of its expert witness that addresses such disclosure.

Because a repository, itself, may run and execute software the usage and distribution of which is managed by the repository, it is unpersuasive that the reference to "repository software" in that portion of the specification discussing "behavioral integrity" (Ex. 1001, 13:8-33) is restricted to software that only manages usage rights. Indeed, in the context of installing software identified as "a new kind or new version of a player," which does

not control usage rights, the specification discusses extracting a copy of the digital certificate for that software (Ex. 1001, 42:31-34), in the same manner that the specification describes requiring a digital certificate in the digital work to ensure behavioral integrity of the repository (Ex. 1001, 13:21-24). Moreover, some repositories are rendering repositories. Ex. 1001, 42:18-21. "Repository software," as used in the specification, is broad enough to cover application software, such as the "player" referenced in column 42, lines 18-21, of the specification, or what ContentGuard refers to as "operating software" which enables the repository to regulate usage rights.

We do not credit the testimony of the expert witness of ContentGuard, Dr. Michael T. Goodrich, in paragraphs 40 and 41 of his declaration (Ex. 2013). In those paragraphs, Dr. Goodrich opines that in his opinion, a person of ordinary skill in the art in 1994 would have understood that the term "repository software" in the '576 patent identifies and refers to the operating software of the repository, and not the software digital works the usage rights of which are controlled by the repository. The testimony is unpersuasive, because they do not account for the disclosure of the specification, discussed above, which conveys that some repositories are themselves rendering depositories which run and execute the software digital works the rights of which they control, such as a new version of a "player."

2.

ContentGuard contends that our construction regarding "behavioral integrity" as "requiring software to include a digital certificate in order to be installed in the repository" is "excessively narrow" because it unnecessarily

requires the inclusion of a "digital certificate" to ensure behavioral integrity. PO Resp. 9-10. According to ContentGuard, in order to maintain behavioral integrity, it is necessary only that the broader purpose of a repository doing what it is supposed to do is satisfied. *Id*. at 10.

ContentGuard's contention that our construction is too narrow is inconsequential to the outcome of this proceeding, because a broader interpretation of "behavioral integrity," would not render inapplicable any teaching of the prior art which was applied under the narrower construction.

We reproduce ContentGuard's argument, here, in more detail:

> The Board's construction is also too narrow because it requires "a digital certificate." After explaining that "[b]ehavioral integrity refers to the integrity in what repositories do" and that "[w]hat repositories do is determined by the software that they execute," the '576 patent says that "[t]he integrity of the software is generally assured only by knowledge of its source." (Ex. 1001, 13:10-11.) Although the specification does say that "behavioral integrity is maintained by requiring that repository software be certified and be distributed with proof of such certification, i.e., a digital certificate," the specification continues by explaining the broader purpose of the certificate. (*Id*., 13:14-17.) "The purpose of the certificate is to authenticate that the software has been tested by an authorized organization, which **attests that the software does what it is supposed to do** and that it does not compromise the behavioral integrity of a repository." (*Id*., 13:17-21 (emphasis added).) So, as long as there is some assurance that "the software does what it is supposed to do," whether by source certification or otherwise, behavioral integrity can be maintained.

PO Resp. 9-10 (emphasis in original).

The breadth argued by ContentGuard is on the extreme end of a spectrum for the meaning of "repository"—whatever ensures a repository does what it is supposed to do. ContentGuard would like to generalize the feature into a generic goal or purpose, entirely removed from any specific means for its implementation. There are several obstacles precluding such an interpretation.

First, the restrictive language in the specification does not permit such an expansive construction. Although it is true that the broadest reasonable construction rule applies for claim interpretation, the construction must be reasonable in light of the specification. In that connection, the specification states: "Behavioral integrity is maintained by *requiring* that repository software be certified and be distributed with proof of such certification, i.e., a digital certificate." Ex. 1001, 13:14-17 (emphasis added).

Second, ContentGuard does not point to any other means, described in the specification, for ensuring behavioral integrity of a repository. The sole disclosure in that regard, as identified by ContentGuard relates to the use of digital certificates. There is no basis to assume, on this record, that digital certificates are representative of all ways for ensuring that a digital work is authentic. Even ContentGuard does not make that assertion. Thus, the scope of disclosure is not commensurate with the breadth for the construction of "repository" desired by ContentGuard.

Third, the general articulation that a repository "does what it is supposed to do" is not accompanied by any well-defined or otherwise recognized standard for making an objective determination in that regard. If

that is the claim construction, the scope of the claims would be uncertain and indeterminable.

We do not credit the testimony of the expert witness of ContentGuard, Dr. Goodrich, that "a person of ordinary skill in the art of 1994 would [have understood] that the '576 patent specification refers to the use of digital certificates as only an exemplary method of preserving the behavioral integrity of a repository." Ex. 2013 ¶ 39. The testimony is unexplained and conclusory. It does not account for the various factors we have considered and discussed above.

B. Alleged Anticipation by EP '139

ZTE contends that claims 18-21, 25-28, and 31-36 are unpatentable under 35 U.S.C. § 102(b) as anticipated by EP '139. Pet. 15-27. ZTE relies on claim charts describing how EP '139 allegedly describes the claimed subject matter, and also on the Declaration of Dr. Vijay K. Madisetti to support its positions. Ex. 1015. To establish anticipation, each and every element in a claim, arranged as is recited in the claim, must be found in a single prior art reference. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008); *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001).

EP '139 discloses a data processing system with a software copy protection mechanism. Ex. 1012, 1:4-6. To provide security, each computer or host that runs a protected software application is associated with a logically and physically secure coprocessor. Ex. 1012, 1:25-29. Figure 1 of EP '139 describes the important components of the software protection

mechanism and how they interact. Ex. 1012, 21:29-31. Figure 1 is reproduced below:

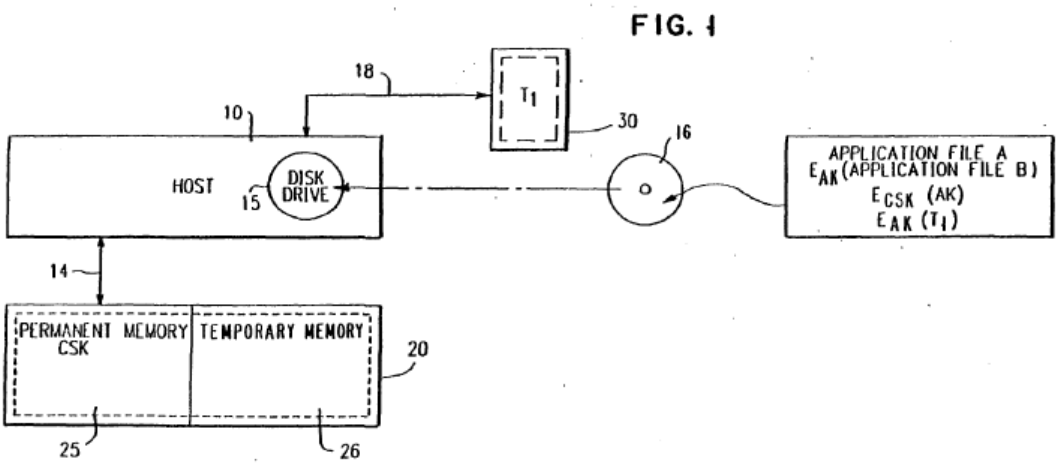

Figure 1 illustrates a composite computing system.

According to the embodiment of Figure 1, EP '139 discloses a software protection mechanism embodied in a composite computing system. Ex. 1012, 21:58-22:5. This composite computer system includes host 10 and coprocessor 20 connected via communication link 14. Ex. 1012, 22:3-6. Coprocessor 20 also includes permanent, non-volatile memory 25 and temporary memory 26. Ex. 1012, 22:19-21. In order to execute a protected application, a user must install a right to execute the application, in the form of a software decryption key, in permanent memory 25. Ex. 1012, 22:22-32. To install this right to execute, the user receives from a software vendor hardware cartridge 30 and distribution disk 16. Ex. 1012, 22:32-36.

In one embodiment, distribution disk 16 stores three files: (1) the protected software application including an encrypted portion; (2) software decryption key AK, encrypted by a different decryption key CSK provided

by the vendor and already stored in coprocessor 20; and (3) token data encrypted by the software decryption key. Ex. 1012, 22:23-27, 36-48. To install the right to execute, coprocessor 20 decrypts the software decryption key in temporary memory, and then verifies that the hardware cartridge is authentic by querying the token data included in the cartridge to determine if they match those in the token data file. Ex. 1012, 23:1-8. Hardware cartridge 30 will contain the token data only if it has not been used. Ex. 1012, 23:8-11.

After verifying that the hardware cartridge is authentic and unused, coprocessor 20 will accept the right to execute and store the software decryption key in permanent memory 25. Ex. 1012, 23:11-16. With access to the software decryption key, the protected application file can be decrypted and stored in temporary memory 26 so that it may be executed by coprocessor 20. Ex. 1012, 23:16-21.

In one embodiment, EP '139 discloses a source composite processor, including source host 10 and coprocessor 20, that may communicate with a sink composite processor, including sink host 110 and sink coprocessor 120. Ex. 1012, 25:49-52. The source and sink processors are interconnected via communication link 200. Ex. 1012, 26:5-6. EP '139 discloses that source coprocessor 20 and sink coprocessor 120 exchange encrypted information. Ex. 1012, 26:10-20. Only coprocessors that are "member[s] of the family" are capable of decrypting and recognizing the information transmitted thereto. Ex. 1012, 26:7-10, 20-23. EP '139 also discloses that the source

coprocessor 20 can encrypt a right to execute a particular software program and send it to the sink coprocessor 120. Ex. 1012, 26:32-35.

As discussed above, "repository" is construed as "a trusted system which maintains physical, communications and behavioral integrity, and supports usage rights." "Physical integrity" is construed as "preventing access to information by a non-trusted system." "Communications integrity" is construed as "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." "Behavioral integrity" is construed as "requiring software to include a digital certificate in order to be installed in the repository." ZTE relies on coprocessor 20 in combination with permanent memory 25 and temporary memory 26 as constituting the claimed "repository." Pet. 20, 25.

EP '139 discloses that coprocessor 20 maintains physical integrity by being "provided with physical security which is effective to prevent mechanical tampering or access to the interior of the coprocessor 20 by a user or a pirate." Ex. 1012, 22:14-17. EP '139 also discloses that coprocessor 20 possesses communications integrity. In order to communicate, proof is required that sink coprocessor 120 is a "member of the family" by exchanging encrypted information via communication link 200. Ex. 1012, 26:5-23.

Behavioral Integrity

ContentGuard argues that EP '139 does not disclose the claimed "repository" because its disclosed system does not exhibit "behavioral integrity." PO Resp. 7-15. The argument has three layers of complexity.

1.

The first relates to ContentGuard's contention that "behavioral integrity" of a repository is directed to, and concerns only, the operating software of the repository, i.e., the software that enables the repository to control the usage rights and distribution of digital works, and not the software digital works managed by the repository themselves. In our claim construction analysis, we already found that contention of ContentGuard unpersuasive.

2.

The second relates to ContentGuard's contention that "behavioral integrity" of a repository does not necessarily require the presence and use of a digital certificate to authenticate the software digital work being installed in a repository. In our claim construction analysis, we also found that contention of ContentGuard unpersuasive.

3.

The third is ContentGuard's contention that software decryption key AK in EP '139, which is associated with the software digital work being sent to coprocessor 20, is not a digital certificate. PO Resp. 14-15. According to ZTE, software decryption key AK in EP '139 amounts to a digital certificate. Reply 2-3. Considering the evidence presented by both parties,

we determine that ZTE has not made an adequate showing to establish, by a preponderance of the evidence, that in the disclosed system of EP '139, the decryption key AK accompanying a software digital work constitutes a digital certificate that authenticates the source of the software.

ZTE's expert, Dr. Vijay K. Madisetti, testified that, in his opinion, the fact that a source coprocessor must encrypt a right-to-execute and transmit that encrypted right-to-execute to a sink coprocessor, as described in column 26, lines 32-35, of EP '139 means the software in EP '139 must include a digital certificate to be installed in a repository. Ex. 1024 ¶ 9. Dr. Madisetti explained that the right-to-execute is required in order for the protected software to be decrypted, stored, and executed. *Id*. (citing Ex. 1012, 23:16-21). On that basis, Dr. Madisetti concludes that "in EPO '139, the AK [decryption key] serves as a digital certificate under the Board's construction as the AK is required in order to install the software in the repository." *Id*.

The reasoning of Dr. Madisetti is tenuous, as the issue is not whether, in some respect, a decryption key under certain overall operating conditions, can "serve as" or substitute for a digital certificate authenticating the source of a software, but whether a decryption key itself "is" a digital certificate. Dr. Madisetti's testimony falls short of stating that decryption key AK would be referred to, or identified by, one with ordinary skill in the art as a digital certificate. As is evident from our discussion of the construction of "behavioral integrity," we are unpersuaded by ContentGuard's contention that a digital certificate is not required, and that anything which accomplishes a similar objective in some way is satisfactory.

ZTE does not account adequately for the fact that, even if decryption of software with the decryption key AK is regarded as authentication of the source of the software, the decryption key, itself, does not authenticate anything. Rather, it has to be applied in a decryption step and it is that process which determines an ascertainable result for further evaluation. Thus, the decryption key is unlike a digital certificate which, by itself, authenticates the source of the software.

Furthermore, it is inadequately explained why decryption indicates authenticity of the software source. That assumes no one tampered with the software while preserving the proper encryption, or that no one created a false or unauthorized version having the proper encryption. The assumptions are speculative in the context of providing security. ZTE identifies in EP '139 a description of several means for checking the authenticity of the software after it has been decrypted. Reply 4-5. For instance, a plain text message recovered on decryption can be checked to see if it matches one actually expected. Ex. 1012, 8:21-39. Such disclosure is evidence that decryption itself does not authenticate.

Insofar as "assurance" means a specifically expressed indication, we credit the testimony of the expert witness of ContentGuard, Dr. Goodrich that "a person of ordinary skill in the art [in 1994] would [have understood] a digital certificate to be an assurance that downloaded software comes from a reputable source, including a measure of tamper resistance." Ex. 2013 ¶ 39 (citing the definition of "digital certificate" from the MICROSOFT COMPUTER DICTIONARY (4th ed. 1999)). An unexpressed and subjective

thought, on the other hand, does not qualify. The decryption key AK, as discussed above, does not meet the requirements of a "digital certificate."

For all of the foregoing reasons, ZTE has not persuaded us that decryption key AK of EP '139 is a digital certificate.

An Authorization Object as Claimed

Claim 18 further recites the steps of "making a request for an authorization object required [sic] to be included within the repository for rendering of the digital content," and "receiving the authorization object when it is determined that the request should be granted." For that authorization object, ZTE relies on EP '139's disclosure of a right-to-execute key, i.e., software decryption key AK, being installed based on the verification of certain token data. Pet. 21-22, 25-26. As already discussed above, ZTE regards coprocessor 20 as the claimed "repository." EP '139 states that "[i]n order for the user to execute a protected application, he must install a right to execute the application in the permanent memory 25; this right to execute is represented by a software decryption key AK." Ex. 1012, 22:27-32.

It is not disputed by ContentGuard that in EP '139, software decryption key AK must be contained in the permanent memory of coprocessor 20 for software to be decrypted and executed. Before accepting the key into permanent memory 25, coprocessor 20 must verify that token data received with the software matches unused tokens in hardware cartridge 30. Ex. 1012, 23:3-8. The authentication is performed by querying the contents of the cartridge. Ex. 1012, 22:46-48, 23:5-8, 20:52-

56. Once the token data is verified, then the software decryption key is stored in permanent memory 25 of coprocessor 20. Ex. 1012, 23:11-16.

Software decryption key AK is first received in the temporary memory of coprocessor 20 and is not moved into the permanent memory of coprocessor 20 unless certain token data which came with the software is determined as valid. Ex. 1012, 23:1-16; Ex. 2013 ¶ 53. Thus, in EP '139, conditioned on a successful test of token data, decryption key AK is moved into where it needs to be, the permanent memory of coprocessor 20, for the software to be executed.

Citing the testimony of its expert witness, Dr. Goodrich (Ex. 2013 ¶ 53), ContentGuard argues that, because ZTE regards coprocessor 20 as the repository, and because temporary memory of coprocessor 20 is a part of the coprocessor, software decryption key AK is already contained within coprocessor 20 as the repository prior to determining whether token data is valid. Thus, according to ContentGuard, the claimed step of "receiving" the authorization object when it is determined that the request for the object should be granted is not satisfied by EP '139.

ZTE argues, on the other hand, that claim 18 does not require "first" receiving the authorization object when it is determined that the request for it should be granted, and, thus, it does not matter that decryption key AK is already contained in coprocessor 20 when it is determined that token data is verified. Reply 7. According to ZTE, because permanent memory 25 is a part of coprocessor 20, moving software decryption key AK into permanent memory 25 is "receiving" software decryption key AK in coprocessor 20.

We are unpersuaded by ZTE's argument, and agree with ContentGuard. Although it is true that claim 18 does not require the authorization object to be "first" received in the repository when it is determined that a request for it should be granted, at least an instance of receiving, as an affirmative act, is necessary. In other words, if not being received for the first time, the authorization object must be received a second, third, or fourth time, and so forth. For an object that already is received, not receiving it another time does not meet the claimed "receiving" step. We agree with ContentGuard that, where coprocessor 20 is the repository and software decryption key AK is the authorization object, moving the key from one part of coprocessor 20 to another part of coprocessor 20 does not meet the requirement of "receiving" the authorization object when it is determined that a request for the object should be granted.

The specification of the '576 patent does not indicate that the named inventor acted as his own lexicographer by setting forth a special meaning for the term "receiving." ZTE does not contend that "receiving" means something other than what it means in the ordinary and common use of the English language, and does not point to any disclosure in the '576 patent that supports its position.

ZTE argues that EP '139 describes that the coprocessor will "accept the right to execute" after verifying that the hardware cartridge is authentic and unused. Reply 7. But the relevant claim term is "receiving," and "accept." There is insufficient evidence that the former encompasses the

latter. In that regard, ZTE cites to the following testimony of its expert witness, Dr. Vijay K. Madisetti: "A person of ordinary skill in the art would reasonably find that the acceptance of the right to execute upon the token test in EP 139 teaches the receiving step of claim 18 under the broadest reasonable interpretation." Ex. 1024 ¶ 15. We do not credit that testimony because it is not accompanied by sufficient explanation. Dr. Madisetti does not explain why there is no difference between "receiving" and "accept," particularly why acceptance by obtaining validation of an object already physically taken into the target location still reasonably would be regarded as "receiving." We conclude that, even under the rule of broadest reasonable interpretation, such a construction is unreasonable.

ZTE further notes that, if the authentication process is unsuccessful, the software decryption key AK will be removed from temporary memory 26 of coprocessor 20. Reply 8. That argument is misplaced, however, because it does not change the fact that if the authentication process is successful, the key as an authorization object already is received in coprocessor 20.

Finally, ZTE argues that, even if it is necessary that the authorization object be "first" received in the repository when it is determined that a request for the object should be granted, another aspect of the disclosure of EP '139 satisfies the claim feature at issue. Reply 8-9. In that regard, ZTE relies on the communication between a source processor and a sink processor for verifying that both are "members of the family." EP '139 discloses that "[a] transfer of a right to execute from one processor to

another is considered safe when the two coprocessors involved are able to identify one another as 'members of the family' and generate a one time only Session Key for their use on that transaction." Ex. 1012, 7:40-45. "Once the Session Key has been generated, it is possible for the coprocessors to transfer rights to execute by encrypting them under the Session Key." *Id*. at 9:3-6.

Thus, according to ZTE, even software encryption key AK as a "right to execute" is not "first" received in the target sink coprocessor until after it has been verified that both coprocessors belong to the same family. That argument, however, was not presented in ZTE's petition. It first was raised in ZTE's Reply. As such, it is inappropriate. ZTE's raising such an argument for the first time in its Reply deprives ContentGuard of an opportunity to respond within the framework of this trial. The argument reasonably cannot be deemed a proper rebuttal to ContentGuard's Patent Owner Response. Rather, it directs focus and attention in a new direction. We decline to consider this new, belated argument in ZTE's Reply.

For all of the reasons discussed above, ZTE has not shown that EP '139 discloses the "receiving" step of claim 18.

Claims 19-21, 25-28, and 31-36 each depend directly or indirectly from claim 18 and, thus, each include the "receiving" step of claim 18. For the same reasons discussed above in the context of claim 18, ZTE has not shown that the "receiving" step of these claims is disclosed in EP '139.

III. CONCLUSION

Petitioner has not proved, by a preponderance of the evidence, that any of claims 18-21, 25-28, and 31-36 of the '576 patent are unpatentable under 35 U.S.C. § 102(b) as anticipated by EP '139.

IV. ORDER

It is

ORDERED that, on this record, claims 18-21, 25-28, and 31-36 of U.S. Patent No. 7,269,576 have not been proved unpatentable; and

FURTHER ORDERED that any party seeking judicial review of this decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER

Jon Beaupre
jbeaupre@brinkshofer.com

Miyoung Shin
mshin@brinkshofer.com

David Bluestone
dbluestone@brinkshofer.com

Rickard DeMille
rdemille@brinkshofer.com

Peter Lee
plee@brinkshofer.com

Lawrence Chen
lchen@brinkshofer.com

For PATENT OWNER

Robert Sterne
rsterne-PTAB@skgf.com

Jon Wright
Jwright-PTAB@skgf.com

Jason Eisenberg
jasone-PTAB@skgf.com