

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

APPLE INC.,  
Petitioner,

v.

CONTENTGUARD HOLDINGS, LLC,  
Patent Owner.

---

Case IPR2015-00446  
Patent 8,370,956 B2

---

Before KARL D. EASTHOM, GLENN J. PERRY, and  
PATRICK R. SCANLON, *Administrative Patent Judges*.

EASTHOM, *Administrative Patent Judge*,

DECISION  
Denying Institution of *Inter Partes* Review  
35 U.S.C. § 314(a), 37 C.F.R. § 42.108

## I. INTRODUCTION

Petitioner, Apple Inc., filed a Petition requesting *inter partes* review of claims 1–18 of U.S. Patent No. 8,370,956 B2 (“’956 patent,” Ex. 1005). Paper 1 (“Pet.”). Patent Owner, ContentGuard Holdings Inc., responded with a Preliminary Response. Paper 10 (“Prelim. Resp.”). We have jurisdiction under 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted “unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” *Id.* at § 314(a).

For the reasons set forth below, we determine that Petitioner does not demonstrate a reasonable likelihood of prevailing in showing the unpatentability of claims 1–18 of the ’956 patent. Accordingly, we deny institution of *inter partes* review.

### A. Related Matters

Petitioner indicates that the ’956 patent was asserted against it by Patent Owner in several lawsuits in U.S. district courts. *See* Pet. 2.

Petitioner filed two other petitions seeking *inter partes* review of the ’956 patent: IPR2015-00447 and IPR2015-00448. Petitioner also filed petitions in Cases IPR2015-00351–358, 399, 400, and 440–458, challenging related U.S. Patent Nos. 6,963,859; 7,225,160; 7,269,576; 7,523,072; 7,774,280; 8,001,053; 8,393,007; and 8,583,556.

*B. The '956 Patent (Ex. 1005)*

The '956 patent describes a system for curbing unauthorized copying and transmission of electronic publications, which it describes as distributing and enforcing usage rights for digital works. *See* Ex. 1005, 1:24–60. “[T]he terms ‘digital work,’ ‘work,’ and ‘content’ refer to any work that has been reduced to a digital representation. . . . includ[ing] any audio, video, text, or multimedia work and any accompanying interpreter (e.g. software) that may be required for recreating the work.” *Id.* at 6:11–15. Usage rights refer to rights granted to a recipient of a digital work that define the manner in which a digital work may be used and distributed. *Id.* at 6:17–20. The disclosed invention provides the owner of a digital work the flexibility to distribute the digital work as desired. *Id.* at 3:66–4:15.

The system attaches usage rights to the digital work, including copies thereof, and stores them in repositories. *Id.* at 6:24–44. A “repository” device, described as being “trusted,” not only stores the digital works, but enforces the usage rights of the digital works, controls access to digital works, bills for access to digital works, and maintains the security and integrity of the digital works stored therein. *Id.* at 6:30–44.

Independent claims 1, 7, and 13 require a recipient device to be “determined to be trusted.” The Specification discloses using an “identification certificate” and a “registration transaction” to determine if a device is trusted: “Identification certificates are the means by which a repository is identified as ‘trustworthy.’” The use of identification certificates

is described below with respect to the registration transaction.” *Id.* at 7:44–48. According to a Glossary in the Specification, an “Identification (Digital) Certificate” is “a signed digital message that attests to the identity of a possessor. Typically, digital certificates are encrypted in the private key of a well-known master repository.” *Id.* at 49:55–59. The Specification also 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.” *Id.* at 13:14–15, 14:27–29.

According to the Specification, a “Registration Transaction[]” is “[t]he protocol used between repositories to establish a trusted session.” *Id.* at 50:5–7. The Specification describes registration transactions further as follows:

The registration transaction between two repositories is described with respect to FIGS. 16 and 17. The steps described are from the perspective of a “repository-1” registering its identity with a “repository-2.” The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1. Referring to FIG. 16, repository-1 first generates an encrypted registration identifier, step 1601 and then generates a registration message, step 1602. A registration message is comprised of an identifier of a master repository, the identification certificate for the repository-1 and an encrypted random registration identifier. **The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository (here repository-1) is a bona fide repository. The identification certificate also**

contains a public key for the repository, **the repository security level** and a timestamp (indicating a time after which the certificate is no longer valid.) The registration identifier is a number generated by the repository for this registration. The registration identifier is unique to the session and is encrypted in repository-1's private key. The registration identifier is used to improve security of authentication by detecting certain kinds of communications based attacks. Repository-1 then transmits the registration message to repository-2, step 1603.

*Id.* at 26:43–67 (emphases added).

As the passage shows, one of the ways that the system determines, or “attests to the fact that the repository . . . is a bona fide repository,” is to include “the repository security level” in the identification certificate. Table 2 in the '956 patent Specification lists different security levels for repositories. *Id.* at 15:1–50.

### *C. Illustrative Claim*

Claims 1, 7, and 13 are independent. Claim 1 is illustrative of the challenged claims:

1. A computer-implemented method of rendering digital content by at least one recipient computing device in accordance with usage rights information, the method comprising:

receiving the digital content by the at least one recipient computing device from at least one sending computing device only if the at least one recipient computing device has been **determined to be trusted** to receive the digital content from the at least one sending computing device;

receiving, by the at least one recipient computing device, a request to render the digital content;

determining, based on the usage rights information, whether the digital content may be rendered by the at least one recipient computing device;

and rendering the digital content, by the at least one recipient computing device, only if it is determined that the content may be rendered by the at least one recipient computing device.

Ex. 1001, 50:55–51:4 (emphasis added).

#### *D. Evidence of Record*

Petitioner relies on the following references and declaration (*see* Pet. 22–36, 48–60):

| <b>Reference or Declaration</b>                                                                                                       | <b>Exhibit No.</b> |
|---------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Declaration of Alan Sherman Regarding U.S. Patent Nos. 6,963,859; 7,523,072; 8,370,956; 8,393,007; 7,269,576 (“Sherman Declaration”). | 1013               |
| Steve R. White and Liam Comerford, <i>ABYSS: A Trusted Architecture for Software Protection</i> , IEEE (1987) (“ABYSS”).              | 1016               |
| Dorothy Elizabeth Robling Denning, <i>CRYPTOGRAPHY AND DATA SECURITY</i> (1983) (“Denning”).                                          | 1017               |
| Hartrick et al., EPO 0567800 A1 (Nov. 3, 1993) (“Hartrick”).                                                                          | 1021               |

#### *E. Asserted Grounds of Unpatentability*

Petitioner asserts that the challenged claims are unpatentable on the following obviousness grounds under 35 U.S.C. § 103(a) (*see* Pet. 48–60):

| <b>Claims</b> | <b>References</b>            |
|---------------|------------------------------|
| 1–18          | ABYSS and Denning            |
| 1–18          | ABYSS, Denning, and Hartrick |

## II. CLAIM CONSTRUCTION

The '956 patent, filed on November 23, 1994, expired on November 23, 2014. *See* Pet. 7; Prelim. Resp. 29. Accordingly, 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. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–17 (Fed. Cir. 2005) (en banc)); *In re Rambus Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (“[T]he Board’s review of the claims of an expired patent is similar to that of a district court’s review.”).

As noted above, the '956 patent’s Appendix provides a “Glossary” defining many of the claim terms. Ex. 1005 at 49:1–50:52. These explicit definitions, and other explicit definitions in the Specification, largely control the construction of many claim terms. The Board previously construed the meaning of certain terms in proceedings involving related patents (Cases IPR2013-00133, -00134, -00137, and -00138). According to Patent Owner and Petitioner, the Eastern District Court of Texas issued similar claim constructions to the Board’s prior constructions. Prelim. Resp. 30 (citing Ex. 2001). The parties largely agree that the Board’s and the District Court’s similar claim constructions should control, with some exceptions that do not appear to be material to a dispute here. *See* Pet. 7–21; Prelim. Resp. 29–36; *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803

(Fed. Cir. 1999) (only terms in controversy need to be construed and only to the extent necessary to resolve the controversy).

Considering the parties' positions, the '956 patent Specification, and the record, we adopt the following constructions for purposes of this Decision only.

*A. "Trusted" (Claims 1, 7, 13)*

According to the Glossary, a "repository is a trusted system in that it maintains physical, communications and behavioral integrity." Ex. 1005 at 50:20–22. Accordingly, the Specification indicates, and the parties agree, that the term "trusted" means "maintains physical, communications, and behavioral integrity, and supports usage rights." See Ex. 1005, 50:20–22; Prelim. Resp. 29–30; Pet. 15–17; Ex. 2001, 13, 15.

*B. Physical, Communications, and Behavioral Integrity—Trusted*

These terms are not in material dispute, but beg interpretation because they serve to define the claim term "trusted." The term "physical integrity" refers to the "integrity of the physical devices themselves. . . . [and] applies both to the repositories and to the protected digital works." Ex. 1005, 12:8–10. Higher security classes may include sensors to preclude tampering on secure cases. See Ex. 1005, 12:10–13. The term "physical integrity" means "preventing access to information by a non-trusted system." See *id.* at 12:17–18; Pet. 18; Prelim. Resp. 30–31. The term "communications integrity" means "only communicates with other devices that are able to present proof that they are trusted systems, for example, by using security

measures such an encryption, exchange of digital certificates, and nonces.”  
See Ex. 1005, 12:34–46; Pet. 18; Prelim. Resp. 30. The term “behavioral integrity” means “requiring software to include a digital certificate in order to be installed in a trusted device.” See Ex. 1005, 12:47–63; Pet. 18; Prelim. Resp. 32.

*C. “Recipient . . . Determined to be Trusted” (Claims 1, 7, 13)*

Claim 1 recites “receiving the digital content by the at least one recipient computing device from at least one sending computing device only if the at least one recipient computing device has been *determined to be trusted* to receive the digital content from the at least one sending computing device.” Claims 7 and 13 recite similar phrases.

Without explicitly setting forth a claim construction for “determined to be trusted,” Petitioner contends that “the sending computing device determines whether the recipient device or apparatus is ‘trusted’ by validating the recipient’s digital certificate.” See Pet. 15 (citing Ex. 1013 ¶¶ B101–103); see also Pet. 16 (similar contention). Petitioner essentially equates the terms “digital certificate” and “identification certificate” and contends that they are “certified by a master device.” See Pet. 14–15. The Glossary supports equating the two by using the terms interchangeably. See Ex. 1005, 49:55–56 (defining “Identification (Digital) Certificate”).

According to the ’956 patent, “[i]dentification certificates are the means by which a repository is identified as ‘trustworthy.’” Ex. 1005, 7:44–46. As discussed above, the Specification states that the “identification

certificate . . . attests to the fact that the repository . . . is a bona fide repository.” *Id.* at 26:57–60.

Therefore, on this record, we construe “determined to be trusted” to mean “using an identification or digital certificate to attest to the fact that a recipient is a trusted device.”

### III. ANALYSIS

Petitioner contends that the combination of ABYSS and Denning, or ABYSS, Denning, and Hartrick, renders claims 1–18 obvious. Pet. 22–60. In support, Petitioner relies on the Sherman Declaration (Ex. 1013). *See id.*

#### *A. ABYSS’s Teachings*

ABYSS (A Basic Yorktown Security System) discloses a system that provides secure software storage and distribution to prevent the theft of intellectual property. Ex. 1016, 38 (Abstract, Introduction).

ABYSS employs “protected processors” which “enable[] the trusted execution of applications.” *Id.* at 50. ABYSS discloses that protected processors may comprise the only processors in a system, or may be part of a larger system that communicates with unprotected processors. *Id.* at 39.

The protected processor is a logically, physically, and procedurally secure unit. It is logically secure, in that an application cannot directly access the supervisor process . . . [or other applications] to violate their protection. It is physically secure . . . in that it is contained in a tamper-resistant package . . . . It is procedurally secure in that the services which move information . . . into and out of the protected processor cannot be used to subvert the protection.

*Id.* at 39.

ABYSS discloses that protected processors execute applications under conditions “embodied in a logical object called a *Right-To-Execute*.” *Id.* The protected processor “enforce[s] [t]hese conditions” (i.e., those in the Right-To-Execute). *Id.* Additional externally-supplied authorization may be required to move the Right-To-Execute between protected processors. *Id.*

### *B. Denning’s Teachings*

Denning provides a graduate level introductory chapter on encryption. Ex. 1017, 1 (Ch. 1 “Introduction,” Sect. 1.1 (“Cryptography)). Denning explains that the reverse of encryption (or enciphering) is decryption (or deciphering). One standard, the Data Encryption Standard (DES), enciphers 64-bit blocks by transposing and substituting characters. In a simple substitution, for example, the Caesar cipher employed by Julius Caesar, the system shifts alphabet positions by  $k=3$ , so that an A would be a D, B would be E, and so on. *Id.* at 2. Denning describes DES as a conventional system. *Id.* at 11.

Encryption schemes require transformations and keys. For example,  $E_k$ , a transformation with ciphering key  $k$ , transforms plain text into encrypted text.  $D_k$ , includes a deciphering key  $k$  and reverses the process to obtain the plain text. *Id.* at 9. In a one-key system, such as DES, both keys must be kept secret to ensure secrecy and authenticity of data. *Id.* at 11. This system works well in computer systems where two communicating devices are “mutually trustworthy.” *Id.* A two-key system, or public-key

encryption system, involves a private deciphering transformation  $D_A$ , known only to user A, and a public enciphering transformation  $E_A$ , which the user registers with a public directory. *Id.* According to Denning, public-key systems can be used to implement digital signatures for authenticity purposes. *Id.* at 14.

### *C. Procedural Defects*

As a threshold matter, the Petition has several significant procedural defects. For instance, a petition for *inter partes* review must “identif[y], in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim.” 35 U.S.C. § 312(a)(3). According to 37 C.F.R. § 42.104(b)(4), a petition for *inter partes* review “must identify . . . [h]ow the construed claim is unpatentable under the statutory grounds” on which the petitioner challenges the claims, and “must specify where each element of the claim is found in the prior art patents or printed publications relied upon.” Rule 42.104(b)(5) requires a petition to “identify[] specific portions of the evidence that support the challenge.” Similarly, 37 C.F.R. § 42.22(a)(2) states that each petition must include “[a] full statement of the reasons for the relief requested, including a detailed explanation of the significance of the evidence including material facts, and the governing law, rules, and precedent.” The Office Patent Trial Practice Guide suggests that parties requesting *inter partes* review should “avoid submitting a repository of all the information that a judge could possibly consider, and instead focus

on concise, well-organized, easy-to-follow arguments supported by readily identifiable evidence of record.” 77 Fed. Reg. 48,756, 48,763 (Aug. 14, 2012).

We agree with the Patent Owner that the Petition fails to satisfy at least the rule requirements. *See* Prelim. Resp. 4–10. The Petition contains vague, nested string citations to broad swaths of the references, the Sherman Declaration, and internal cross-references to whole sections of the Petition. *See, e.g.*, Pet. 48–49 (discussing the preamble of claim 1, and citing *inter alia*, “[Pet.] § IV.A.1, A.3; Ex. 1016 at 38–40, 43–45; Ex. 1013 at ¶ C18–22 and “Ex. 1016 at 38–40, 42, 49, 50; [Pet.] § IV.A.3–4; Ex. 1013 at ¶ C106–26”).

Similar to the discussion of the preamble, the analysis of (what the Petition identifies as) element c of claim 1 spans about one page of the Petition, but cites to 34 paragraphs of the Sherman Declaration and at least eight other pages of internal sections of the Petition. *See* Pet. 49–50 (citing Pet. §§ III.D.4, IV.D.2, IV.D; IV.E.2; Ex. 1013 ¶¶ C153–170, C81–89, C118–24).<sup>1</sup> This count does not include the further internal citations and cross-references contained in the cross-cited portions of Petition. The same problem continues for the remaining claim elements. For example, although

---

<sup>1</sup> The Petition incorrectly or vaguely cites “[s]ee § E.2; Ex. 1013 at 153–170”—neither of which exist—instead of (what probably should be) a citation to “Pet. § IV.E.2.; Ex. 1013 ¶¶ C153–170.”

the unpatentability analysis of the last claim element, element e, involves eight lines in the Petition, it cites 18 paragraphs of the Sherman Declaration, 6 pages of ABYSS, and 6 other pages of the Petition. *See* Pet. 51. These nested citations to so much of the record obscure what exactly Petitioner relies upon as teaching or suggesting the claim elements.

The Petition's labyrinthine structure exacerbates the clarity problems caused by the nested citations. The Petition's unpatentability analysis divides into roughly five sections. First, the Petition presents a synopsis describing what Petitioner contends each of the three principal references relied upon in the Petition generally discloses. *See* Pet. 22–36. Although this section quotes from each reference, it also includes extensive citations to the Sherman Declaration and various characterizations of the references. *See, e.g., id.* at 24 (citing Ex. 1016, 38–40, 43–45, 49, 50; Ex. 1013 ¶¶ C6, C34–45, C74, C75, C147, C148). Second, the Petition constructs a Denning “implemented” ABYSS system using certain encryption techniques (public-key encryption (“PKI”)) taught in Denning, which Petitioner contends would be incorporated “into at least four different elements of the ABYSS system.” *See* Pet. 36, 37–40. Third, the Petition then describes the “operation” of the “implemented” system. *See id.* at 39–41 (emphases omitted). Fourth, the Petition discusses how, based on the “operation” of the “implemented” system, the implementation discloses “repositories” and “usage rights,” as Petitioner construes those terms. *See id.* at 42–46. Fifth, the Petition maps

this “operation[]” of the “implementation” of ABYSS onto the claims. *See id.* at 48–56.

This mapping relies on all the previous summaries and descriptions. *Id.* Thus, the unpatentability analysis relies on Petitioner’s description and characterization of a hypothetical operation of a hypothetical implementation of a combined system. The resultant approach renders the final unpatentability analysis two or three levels removed from the actual disclosure of the references. Petitioner’s approach completely blurs the line between the actual teachings, Petitioner’s modifications to the teachings, and Petitioner’s characterizations of those teachings. This approach improperly shifts the burden of deciphering Petitioner’s arguments onto Patent Owner and the Board.

The lack of clarity in the Petition is further compounded by the improper incorporation by reference of the Sherman Declaration. The Petition includes many conclusory statements that cite to broad swathes of the lengthy Sherman Declaration.<sup>2</sup> Without referring entirely to the Sherman Declaration, many sections of the Petition would be unintelligible. The Petition’s practice of citing multiple pages of the Sherman Declaration

---

<sup>2</sup> The Sherman Declaration comprises 470 pages (not including a four page list of references). It relates to patents and references not at issue in this proceeding. The portions relating to this proceeding encompass about 100 pages (not including a general discussion that is about another 100 pages in length).

to support conclusory statements and more generally, using the Sherman Declaration to vastly expand its thin analysis and reasoning, violates Board rules in at least two respects. First, this practice amounts to an impermissible incorporation by reference. *See* 37 C.F.R. § 42.6(a)(3) (“Arguments must not be incorporated by reference from one document into another document.”); *Cisco Sys., Inc. v. C-Cation Techs., LLC*, Case IPR2014-00454, slip op. at 7–10 (PTAB Aug. 29, 2014) (Paper 12) (informative). This incorporation by reference from the 470 page Sherman Declaration into the Petition “serves to circumvent the [60-]page limit[] imposed on petitions for *inter partes* review, while imposing on our time by asking us to sift through [hundreds of] pages of [the] Declaration (including numerous pages of claim charts) to locate the specific [relevant] arguments.” *Cisco Sys., Inc.*, IPR2014-00454, at 10 (Paper 12) (informative); *see* 37 C.F.R. § 42.24(a)(1)(i).

Arguments and information that are not presented and developed in the Petition, and instead are incorporated by reference to the Sherman Declaration, are not entitled to consideration. Second, the Petition’s consistent citation to voluminous portions of the Sherman Declaration, which generally include additional internal cross-references, runs afoul of the particularity and specificity required of supporting evidence under our governing rules. *See* 37 C.F.R. §§ 42.22(a)(2), 42.104(b)(4)–(5).

In addition, the record contains 63 Exhibits totaling roughly 14,000 pages, most of which the Petition does not cite. As noted previously, The

Office Patent Trial Practice Guide cautions that petitioners should “avoid submitting a repository of all the information that a judge could possibly consider, and instead focus on concise, well-organized, easy-to-follow arguments supported by readily identifiable evidence of record.” 77 Fed. Reg. at 48,763. For the foregoing reasons, the Petition widely misses that mark.

Based on the deficiencies addressed above, the Petition fails to (1) specify sufficiently where the limitations of the challenged claims are taught or suggested by ABYSS or Denning and (2) provide a sufficiently detailed explanation of the significance of the citations to these references and the Sherman Declaration—as required under 37 C.F.R. §§ 42.22(a)(2) and 42.104(b)(4)–(5).

*D. Defects in the Proffered Obviousness Analysis*

Even considering the merits of the Petition, Petitioner’s analysis of the asserted grounds of obviousness is deficient. The Petition’s obviousness analysis does not provide sufficient information to perform a proper *Graham* analysis, lacks sufficient articulated reasons with rational underpinning to support the proposed modifications, and fails to analyze the claim elements properly.

*1. Insufficient Information for Graham Analysis*

A patent claim is unpatentable as obvious under 35 U.S.C. § 103(a) if “the differences between” the claimed subject matter and the prior art “are such that the subject matter, as a whole, would have been obvious at the time

the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” 35 U.S.C. § 103(a); *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).<sup>3</sup> The legal conclusion of obviousness is resolved on the basis of underlying factual determinations, including (1) “the scope and content of the prior art,” (2) “differences between the prior art and the claims at issue,” (3) “the level of ordinary skill in the pertinent art,” and (4) any “secondary considerations,” or objective indicia, of nonobviousness. *Graham v. John Deere Co. of Kan. City*, 383 U.S. 1, 17–18 (1966). These underlying factual determinations “must be considered by the trier of fact” in an obviousness analysis. *ATD Corp. v. Lydall, Inc.*, 159 F.3d 534, 546 (Fed. Cir. 1998).

As Patent Owner points out, the Petition fails to identify sufficiently the differences between any claim of the ’956 patent and the asserted prior art references, ABYSS, Denning, and Hartrick. See Prelim. Resp. 6–7, 42–44; Pet. 22–60. Rather than address these differences, the Petition creates a hypothetical ABYSS-Denning system—based on how a person of ordinary skill in the art allegedly “would” or “could” do—in an “Operation of the Implemented System” analysis divorced from the language of the ’956 patent claims. See Pet. 39–42 (emphasis omitted). The Petition then argues,

---

<sup>3</sup> The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011), revised 35 U.S.C. § 103, effective March 16, 2013. Because the ’956 patent was filed before March 16, 2013, references and citations to § 103 in this Decision are to the pre-AIA version.

in conclusory fashion, that this hypothetical system meets each of the limitations of the claims. *See id.* at 48–60. This analysis—which compares the challenged claims to a hypothetical integrated system that allegedly implements elements of both ABYSS and Denning as well as the knowledge of one of ordinary skill in the art—obscures any comparison of the individual prior art references to the claim limitations. It does not explain with any particularity which claim limitations are absent from ABYSS or Denning. *See* Prelim. Resp. 6–7, 42–44. Therefore, the Petition fails to provide sufficient information regarding its proffered ground of unpatentability, and fails to present a proper *Graham* analysis as required to show that the challenged claims are unpatentable.

Accordingly, we determine that the Petition does not show a reasonable likelihood that Petitioner would prevail in showing that the challenged claims would have been obvious over ABYSS and Denning. *See Apple Inc. v. SmartFlash LLC*, Case CBM2015-00029, slip op. at 16–18 (PTAB May 28, 2015) (denying institution of an asserted obviousness ground based on Petitioner’s failure to explain adequately any differences between the asserted prior art and the claimed invention); *Liberty Mut. Ins. Co. v. Progressive Casualty Ins. Co.*, Case CBM2012-00003, slip op. at 3 (PTAB Oct. 25, 2012) (Paper 7) (representative) (“A petitioner who does not state the differences between a challenged claim and the prior art, and relies instead on the Patent Owner and the Board to determine those differences . .

. risks having the corresponding ground of obviousness not included for trial for failing to adequately state a claim for relief.”).

2. *Lack of Rationale to Combine and Improper Hindsight*

“[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). The reason for this is that “[w]hile the Supreme Court made clear that a mechanical application of the teaching-suggestion-motivation test, requiring an explicit teaching in the prior art, is inappropriate, ‘[w]e must still be careful not to allow hindsight reconstruction of references to reach the claimed invention without any explanation as to how or why the references would be combined to produce the claimed invention.’” *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1368 (Fed. Cir. 2012) (quoting *Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 n.3 (Fed. Cir. 2008)); *see also KSR*, 550 U.S. at 421 (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”); *Graham*, 383 U.S. at 36 (warning against a “temptation to read into the prior art the teachings of the invention in issue” and instructing courts to “guard against slipping into use of hindsight” (citation omitted)). Thus, “[c]are must be taken to avoid hindsight reconstruction by using ‘the patent in suit as a guide through the maze of prior art references, combining the right references in the right way so as to

achieve the result of the claims in suit.”” *Grain Processing Corp. v. Am. Maize–Prods. Co.*, 840 F.2d 902, 907 (Fed. Cir. 1988) (quoting *Orthopedic Equip. Co. v. United States*, 702 F.2d 1005, 1012 (Fed. Cir. 1983)).

As discussed above, Petitioner reads the claims onto a proposed hypothetical ABYSS-Denning system. *See* Pet. 38–60. Although Petitioner frames the hypothetical ABYSS-Denning system as created by four main modifications, each of these modifications includes what appear to be additional modifications about what the hypothetical system “could” do, which neither reference discloses, and which the Petition does not support with sufficient reasoning or citation. *See* Pet. 36–39 (modifications); *see, e.g.*, Pet. 40–41 (reasoning that a “vendor could restrict distribution to processors that had a digital certificate issued by a particular authority,” and “[t]he vendor also could specify as a condition” further changes) (citing Pet. “§ IV.D.1; Ex. 1013 at ¶ C83–89, C113”). Considering the proposed changes together, which are devoid of a clear reference to claim limitations, the Petition lacks adequate reasoning, with rational underpinning, to show sufficiently that a person of ordinary skill would have combined the teachings of ABYSS and Denning to reach the hypothetical ABYSS-Denning system and render the claims obvious. In other words, the Petition fails to explain sufficiently why a person of ordinary skill would simultaneously make all of the particular proposed changes and implementation choices. Moreover, the mere fact that individual changes might have been obvious does not make doing all of the changes at once

obvious. *See In re Irani*, 427 F.2d 806, 809 (CCPA 1970) (“Obviousness, however, must not be judged by hindsight, and a ‘little modification’ can be a most unobvious one.”).

The extent of the proposed modifications and the thin reasoning proffered for each modification suggests that the Petition improperly uses Patent Owner’s claims as a guide in constructing a system loosely based on ABYSS and Denning. *See Plantronics, Inc. v. Aliph, Inc.*, 724 F.3d 1343, 1355 (Fed. Cir. 2013) (“Where, as here, the necessary reasoning is absent, we cannot simply assume that ‘an ordinary artisan would be awakened to modify prior art in such a way as to lead to an obviousness rejection.’ It is in such circumstances, moreover, that it is especially important to guard against the dangers of hindsight bias.” (citation omitted)); *see also W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1552 (Fed. Cir. 1983) (“The result is that the claims were used as a frame, and individual, naked parts of separate prior art references were employed as a mosaic to recreate a facsimile of the claimed invention. At no point did the district court, nor does Garlock, explain why that mosaic would have been obvious to one skilled in the art . . .”). The Petition’s analysis, infected with impermissible hindsight, cannot form the basis of a proper obviousness finding. *See KSR*, 550 U.S. at 421 (“A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.”); *Graham*, 383 U.S. at 36 (warning against a “temptation to

read into the prior art the teachings of the invention in issue” and instructing courts to “guard against slipping into use of hindsight” (citation omitted)).

In sum, we are not persuaded that the Petition shows sufficiently why one of ordinary skill in the art—without improper hindsight—would have combined ABYSS and Denning to reach the challenged claims. Therefore, we determine that the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that any of the challenged claims would have been obvious over ABYSS and Denning.

### *3. Particular Claim Elements*

Independent claims 1, 7, and 13 recite similar limitations and are similar in scope. Accordingly, this discussion focuses on claim 1.

Claim 1 recites “receiving the digital content by the at least one recipient computing device from at least one sending computing device only if the at least one recipient computing device has been determined to be trusted to receive the digital content from the at least one sending computing device.” Ex. 1005, 50:58–62. Petitioner generally relies on modifying ABYSS’s protected processor supervisor system so that it employs selected aspects of public key authentication techniques described in Denning. *See* Pet. 33, 36–39, 42–45, 48–49.

Purporting to address this claim element, Petitioner sets forth the following:

c) receiving “digital content by . . . recipient computing device

from . . . sending computing device only if [it] . . . has been determined to be trusted to receive the digital content”

Because repositories are the only types of devices that are “trusted” and able to enforce rights in the ’956 patent scheme, the “*recipient computing device [apparatus]*” and the “*sending computing device*” must be repositories. See § III.D.4. Each ABYSS protected processor, modified by Denning, is a “repository.” See § E.2; Ex. 1013 at ¶ 153-70.

In the PKI implemented ABYSS scheme, each workstation with a protected processor (“*repository*”) is able to communicate with other protected processors (also “*repositories*”) over a network. See § IV.D.2; Ex. 1016 at 44, 49, 50; Ex. 1017 at 178-79; Ex. 1013 at ¶ C81-89. For example, the workstation’s protected processor (“*recipient computing device*”) will attempt to establish a secure connection with the file server’s protected processor (“*sending computing device*”) by sending its digital certificate to the file server. Ex. 1016 at 49; Ex. 1017 at 178-79; Ex. 1013 at ¶ C118-21. The file server’s protected processor will validate the digital certificate by determining if it was issued by the group’s certificate authority (“*has been determined to be trusted to receive digital content from at least one sending computing device*”). Ex. 1013 at ¶ C118-21; see § III.D.4, IV.D. If the digital certificate is valid, the file server’s protected processor will determine if copies are available, and if so, transmit a copy of the software and Right-To-Execute to the workstation’s protected processor (“*receiving the digital content by the at least one computing device from at least one sending computing device*”). See Ex. 1016 at 49; Ex. 1017 at 178-179; § IV.D.2; Ex. 1013 at ¶ C122-24.

Pet. 49-50.

This passage reads a claim limitation onto a hypothetical repository, the “ABYSS protected processor, modified by Denning.” Pet. 49. The passage also states that “the workstation’s protected processor (“*recipient computing device*”) will attempt to establish a secure connection with the file server’s protected processor (“*sending computing device*”) by sending its digital certificate to the file server.” Pet. 50 (citing Ex. 1016, 49; Ex. 1017 at 178–79; Ex. 1013 ¶¶ C118–21). Contrary to this assertion, Petitioner’s citations to the record do not support that ABYSS’s workstations in the disclosed file server example (disclosed by ABYSS as a *software lending library*) each have protected processors or send digital certificates. Ex. 1016, 49. Rather, at the cited page, ABYSS describes a file server that has a protected processor and connects to a large number of workstations to obtain “significant economies” in a “local area network,” but that page does not disclose that each workstation in that local area network scenario includes a protected processor. *Id.* Also, ABYSS generally contemplates systems that include both protected and unprotected processors (and encryption for security thereof). *See id.* at 39–40.

The quoted passage in the Petition also states that “in the PKI implemented ABYSS scheme, . . . [t]he file server’s protected processor will validate the digital certificate by determining if it was issued by the group’s certificate authority (“*has been determined to be trusted to receive digital content from at least one sending computing device*”).” *Id.* at 50 (citing Ex. 1013 ¶ C118–21; Pet. § III.D.4, IV.D). However, contrary to this

quoted Petition passage, ABYSS does not disclose using digital certificates in the manner described, if at all. Even if a hypothetical “PKI implemented ABYSS scheme” uses a digital certificate and somehow uses “the group’s certificate authority” according to Petitioner’s hypothetical modifications elsewhere in the Petition, the Petition does not indicate clearly how validating a digital certificate by a file server from a workstation’s processor (even if it is protected) determines that the work station’s processor is “trusted” to receive digital content from the file server’s protected processor, as claim 1 requires. *See id.*

In other words, as discussed above, the parties agree that the term “trusted” requires communications integrity, behavioral integrity, and physical integrity. *See* Section II *supra*; Ex. 1005, 12:8–63; Pet. 17–18; Prelim. Resp. 30. The Petition fails to explain clearly how even a hypothetical PKI implemented ABYSS scheme determines (i.e., “attest[s] to the fact”) that a workstation’s protected processor has behavioral integrity. *See supra* Section II.E.

The term “behavioral integrity” means “requiring software to include a digital certificate in order to be installed in a trusted device.” *See* Ex. 1005, 12:47–63; Pet. 18; Prelim. Resp. 32. According to the passage quoted above, Petitioner contends that “if copies are available,” the file server’s protected processor “transmit[s] a copy of the software and Right-To-Execute to the workstation’s protected processor.” Pet. 50. Setting aside the communications and physical integrity, which a trusted device requires,

but the quoted passage does not describe, the passage also does not describe behavioral integrity. *See* Pet. 49–50. In the relied-upon hypothetical lending library example, behavioral integrity would require transmitting, from the file server (and elsewhere), a digital certificate with each copy of software. The passage does not describe how validating a previously sent digital certificate (as set forth in the passage) from a workstation, constitutes, or renders obvious, determining (i.e., attesting to the fact) that hypothetical workstations in ABYSS’s modified system have behavioral integrity—and thereby attest to the fact that they would always require a digital certificate in each copy of a received software item. Rather than using a digital certificate authorization process, let alone such a process in the manner that Petitioner contends, ABYSS uses a token system, and generally discloses that “[t]here are many possible authorization processes, including ones in which the user’s protected processor must communicate with a processor capable of cryptographic transactions, in order to receive proper authorization.” Ex. 1016, 44 (emphasis added).

At the cited paragraphs to the Sherman Declaration in the quoted Petition passage (Pet. 49–50), Dr. Sherman refers back to earlier passages in the Sherman Declaration to support a description about a hypothetical “certificate exchange process.” *See, e.g.*, Ex. 1013 ¶ C119 (citing ¶¶ A148–52 and ¶¶ C29, C51). The cited paragraphs fail to describe in a clear fashion the differences between claim elements and ABYSS. For example, Dr. Sherman states that

ABYSS explains a protected processor determines whether another device is an authorized protected processor by verifying that the device has an authorized supervisor key, or digital certificate. . . . By verifying that the digital certificate was issued by a trusted authority, the file server determines the workstation is authorized.

Ex. 1013 ¶ C121 (citing Ex. 1016, 42, 43, 47, 48). Contrary to this testimony, which is similar to the quoted passage above (Pet. 49–50), ABYSS does not disclose using digital certificates in the manner described, if at all. The cited testimony also does not address determining if a protected processor has or requires behavioral integrity in a clear fashion, if at all (and even if it did, would amount to improper incorporation-by-reference, for reasons discussed above). Again, this type of analysis renders the Petition unclear by obscuring what ABYSS discloses and what Petitioner relies upon for obviousness.

Based on the foregoing discussion, we determine that Petitioner has not demonstrated a reasonable likelihood that ABYSS and Denning render obvious independent claim 1, and similarly, independent claims 7 and 13. Petitioner’s showing with respect to claims 2–6, 8–12, and 13–18, which depend from one of the independent claims, does not cure the deficiencies described with respect to the independent claims.

#### *E. Additional Grounds*

Petitioner also argues that claims 1–18 would have been obvious over combination of ABYSS, Denning, and Hartrick. Pet. 57–60. Petitioner’s reliance on Hartrick does not cure the deficiencies noted above.

#### IV. CONCLUSION

For all the reasons discussed above, we determine that the Petition fails to show there is a reasonable likelihood that Petitioner would prevail with respect to at least one of the claims challenged in the Petition. *See* 35 U.S.C. § 314(a); 37 C.F.R. § 42.8(b)(2).

#### V. ORDER

Accordingly, it is

ORDERED that the Petition is denied and no trial is instituted.

IPR2015-00446  
Patent 8,370,956 B2

For PETITIONER:

Jeffrey P. Kushan  
Michael R. Franzinger  
SIDLEY AUSTIN LLP  
jkushan@sidley.com  
mfranzinger@sidley.com  
iprnotices@sidley.com

PATENT OWNER:

Nicholas T. Peters  
Timothy P. Maloney  
FITCH, EVEN, TABIN & FLANNERY LLP  
ntpete@fitcheven.com  
tpmalo@fitcheven.com

Robert A. Cote  
MCKOOL SMITH, PC.  
rcote@mckoolsmith.com