

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

IPR2020-01123
Patent 6,157,721

Before MICHAEL R. ZECHER, NABEEL U. KHAN, and
CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

KHAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. *Background and Summary*

Dolby Laboratories, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting an *inter partes* review of claims 5, 9, and 29 of U.S. Patent No. 6,157,721 (Ex. 1001, “the ’721 patent”). Intertrust Technologies Corporation (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”). With its Preliminary Response, Patent Owner filed a statutory disclaimer, disclaiming claim 5 of the ’721 patent. *See* Ex. 2019. Petitioner and Patent Owner filed additional briefing with our authorization. *See* Papers 8, 9. On January 6, 2021, upon consideration of the Petition, Preliminary Response, the additional briefing, and the statutory disclaimer of claim 5, we instituted review to determine the patentability of claims 9 and 29 (“the challenged claims”) but did not institute review of claim 5. Paper 10 (“Dec. Inst.”).

After institution, Patent Owner filed a Patent Owner Response (Paper 18, “PO Resp.”), Petitioner filed a Reply (Paper 22, “Pet. Reply”), and Patent Owner filed a Sur-Reply (Paper 24, “PO Sur-reply”). An oral hearing was held on October 5, 2021, and the hearing transcript is included in the record. Paper 32 (“Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Final Written Decision, issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73 (2019), addresses issues and evidence raised during the *inter partes* review. For the reasons that follow, Petitioner demonstrates by a preponderance of the evidence that claims 9 and 29 of the ’721 patent are unpatentable.

B. Related Matters

The parties identify four related district court cases involving the '721 patent: (1) *Dolby Laboratories, Inc. v. Intertrust Corporation*, No. 3:19-cv-03371 (N.D. Cal.); (2) *Intertrust Technologies Corporation v. AMC Entertainment Holdings, Inc.*, No. 2:19-cv-00265 (E.D. Tex.); (3) *Intertrust Technologies Corporation v. Cinemark Holdings, Inc.*, No. 2:19-cv-00266 (E.D. Tex.); and (4) *Intertrust Technologies Corporation v. Regal Entertainment Group*, No. 2:19-cv-00267 (E.D. Tex.). *See* Pet. 7; Paper 5, 1.

C. The '721 Patent

The '721 patent is titled “Systems and Methods Using Cryptography to Protect Secure Computing Environments,” and the application giving rise to the '721 patent was filed on August 12, 1996, and issued on December 5, 2000. Ex. 1001, codes (21), (22), (54). The application giving rise to the '721 patent is the only patent application referenced for the benefit of a prior filing date under 35 U.S.C. § 120 and the '721 patent has no term extensions. Accordingly, the term of the '721 patent has expired. *See* 35 U.S.C. § 154(a)(2) (2018).

The '721 patent is directed to systems and methods for protecting secure processing environments or other secure execution spaces from unauthorized and potentially harmful “load modules,” other “executables,” or associated data. Ex. 1001, 1:19–28, 4:51–56. To accomplish this, one or one or more trusted verifying authorities may validate load modules or other executables by analyzing or testing them, and a verifying authority may digitally “sign” and “certify” those load modules or other executables it has

verified (for example, using a public key based digital signature or certificate based thereon). *See id.* at 4:61–67.

Figure 14 of the '721 patent is reproduced below.

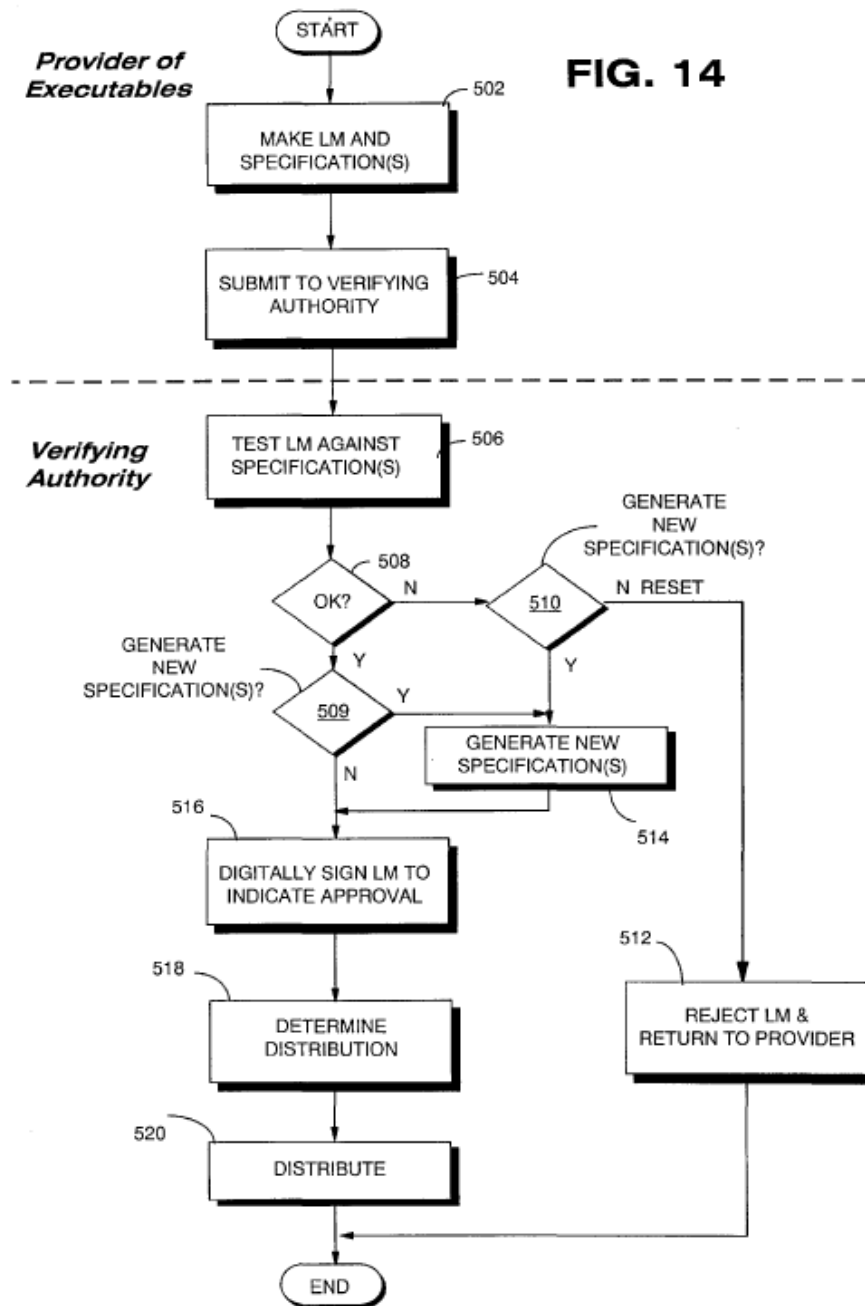


Figure 14 depicts an example of a process according to one embodiment of the '721 patent. Ex. 1001, 8:7–10, 20:26–28. As shown in Figure 14, a load module provider may manufacture a load module and its specifications (step

502) and submit it to a verifying authority for verification (step 504). *Id.* at 20:28–32. The verifying authority may analyze, test or otherwise validate the load module and determine whether it satisfies the specifications (step 506). *Id.* at 20:32–36. If it determines that the load module satisfies its specifications, the verifying authority may determine whether it is authorized to generate one or more new specifications (step 508). *Id.* at 20:37–40. If it is authorized and this function has been requested (step 509), the verifying authority may generate the new specifications and associate them with the load module (step 514). *Id.* at 20:40–43.

If the load module fails the test, the verifying authority may still create new specifications that conform to the load module performance (step 514) if it is authorized to do so, and it would be desirable (step 510). Ex. 1001, 20:44–49, 20:52–56. Otherwise, the verifying authority may decide not to create the new specifications, the load module may be rejected and returned to the provider, and the process ends (step 512). *Id.* at 20:49–52. For those load modules in which new specifications have been generated or created, the verifying authority may digitally sign the load module to indicate approval by applying or selecting appropriate digital signatures (step 516). *Id.* at 20:58–20:63. The verifying authority may then determine the distribution of the load module (step 518) and distribute the appropriate information to a value chain (step 520). *Id.* at 20:63–21:7.

Figure 3 of the '721 patent is reproduced below.

FIG. 3 Before Protected Processing Environment Uses A Load Module, It Checks To See If Load Module Has Been Verified

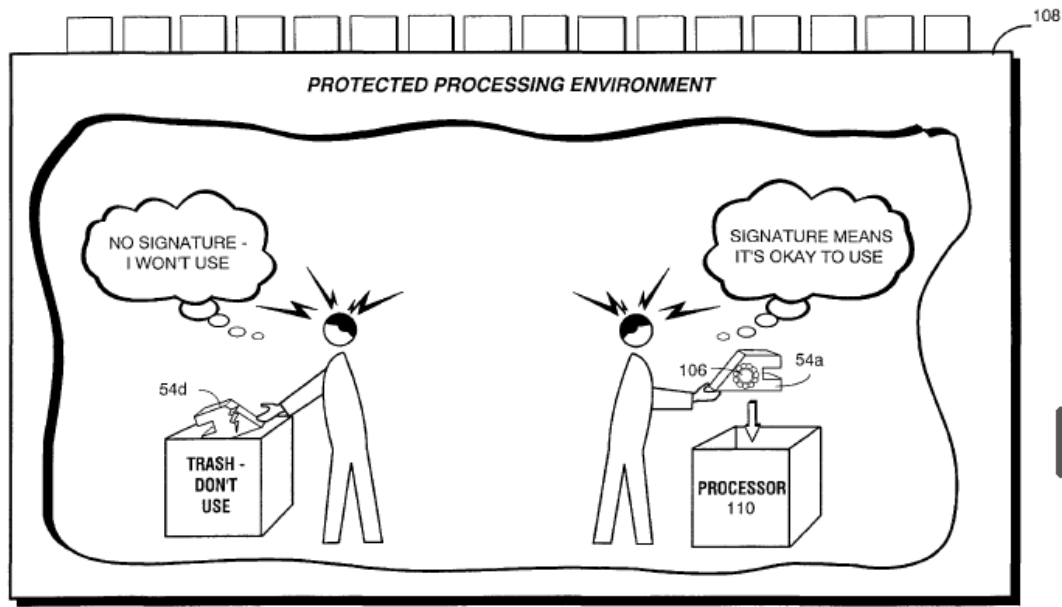


Figure 3 of the '721 patent depicts how a protected processing environment 108 may distinguish load modules 54a that have been approved by the verifying authority from load modules 54 that have not been approved. Ex. 1001, 7:41–44, 9:52–55. The protected processing environment may distinguish between authorized and unauthorized load modules by examining the load module to see whether it bears the seal (e.g., seal 106) of the verifying authority, which may comprise one or more “digital signatures.” *Id.* at 9:53–54, 9:58–61. Protected processing environment 108 may execute load module 54a with its processor 110 only if the load module bears the verifying authority’s signature 106. *Id.* at 9:61–64. Protected processing environment 108 may discard and not use any load module 54 that does not bear this signature 106. *Id.* at 9:64–66. In this way, protected processing environment 108 may securely protect itself against unauthorized

load modules 54 such as defective load module 54*d* made by a disreputable load module provider. *Id.* at 9:66–10:3.

Figure 6 of the '721 patent is reproduced below.

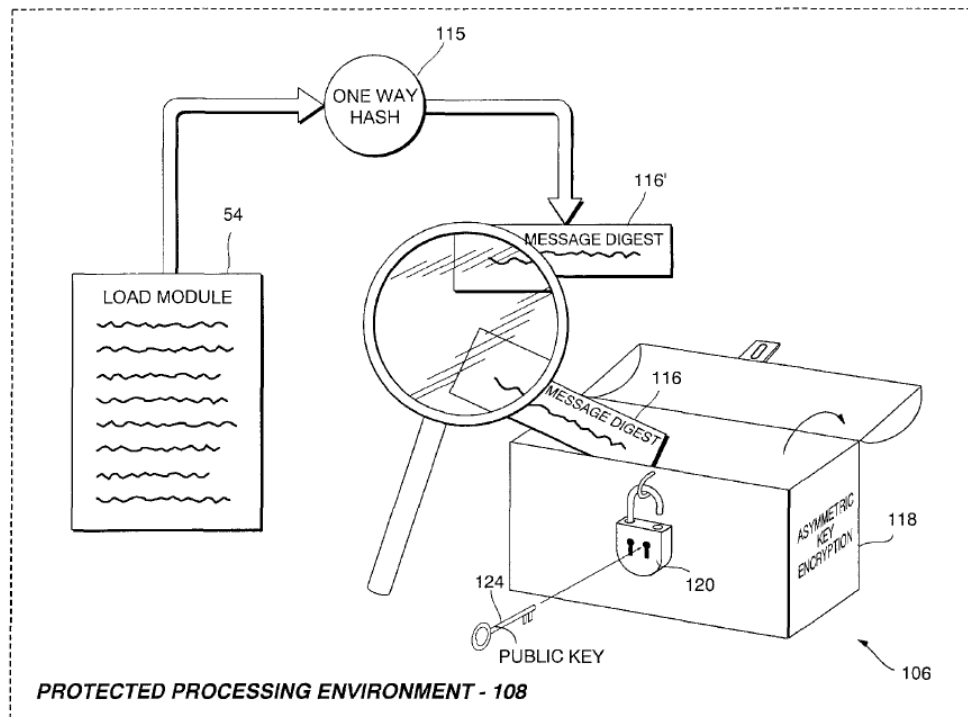


FIG. 6 Authenticating a Digital Signature

Figure 6 of the '721 patent depicts how protected processing environment 108 may “authenticate” a digital signature created by the verifying authority. Ex. 1001, 7:49–52, 13:60–62. As shown in Figure 6, second key 124 and the one-way hash transformation function 115 are securely provided to protected processing environment 108. *Id.* at 13:62–64. Public key cryptography allows second key 124 to be made public without compromising first key 122. *Id.* at 13:66–14:1. However, in the example shown in Figure 6, protected processing environment 108 preferably keeps public second key 124 secret. *Id.* at 14:1–5. This enhances security by greatly complicating an attacker’s job of generating bogus digital signatures

106 and by foreclosing “the significant threat that the owner of protected processing environment 108 himself may attack the environment.” *Id.* at 14:1–9, 14:23–26; *see also id.* at 14:9–22, 14:26–38 (discussing how the owner could replace public key 124 with his own substitute public key and force protected processing environment 108 to execute load modules of his own design).

Load module 54 and its associated digital signature 106 are then delivered to protected processing environment 108, which applies one way hash transformation function 115 on load module 54 and generates message digest 116'. Ex. 1001, 14:39–48. Protected processing environment 108 then decrypts digital signature 106 using second key 124. *Id.* at 14:49–50. This process includes opening strongbox 118 to retrieve message digest 116, which verifying authority 100 placed in strongbox 118 when creating digital signature 106. *Id.* at 13:30–35, 14:50–52. Protected processing environment 108 then compares message digest 116 with message digest 116'—which should be identical. *Id.* at 14:52–57. If they do not match, then either digital signature 106 is not authentic or load module 54 has been changed, so protected processing environment 108 rejects load module 54. *Id.* at 14:57–60.

D. Illustrative Claims

Claims 9 and 29 are independent and recite nearly identical limitations, with claim 9 reciting “load modules” whereas claim 29 recites “executables.” *Compare* Ex. 1001, 22:5–15, *with id.* at 24:10–21.

Claim 9 is reproduced below.

9. A method of distinguishing between trusted and untrusted load modules comprising:

(a) receiving a load module,

(b) determining whether the load module has an associated digital signature,

(c) if the load module has an associated digital signature, authenticating the digital signature using at least one public key secured behind a tamper resistant barrier and therefore hidden from the user; and

(d) conditionally executing the load module based at least in part on the results of authenticating step (c).

Ex. 1001, 22:5–15.

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 9 and 29 are unpatentable based on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
9, 29	102(a) ¹	Arnold ²
9, 29	103(a)	Arnold
9, 29	103(a)	Chang ³ , Stefik ⁴

In addition, Petitioner relies on the Declaration of Sandeep Chatterjee, Ph.D. (Ex. 1002) in support of the asserted grounds of unpatentability. *See generally* Pet.; Pet. Reply. Patent Owner relies on the Declaration of Dr. Markus Jakobsson (Ex. 2027) in support of Patent Owner’s Response. *See generally* PO Resp.; Sur-reply.

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103, effective March 16, 2013. Because the application from which the ’721 patent issued claims priority to applications filed before this date, the pre-AIA versions of §§ 102 and 103 apply.

² EP 0706275 A2, published April 10, 1996 (Ex. 1004, “Arnold”).

³ US 5,724,425, issued March 3, 1998 (Ex. 1005, “Chang”).

⁴ US 5,715,403, issued February 3, 1998 (Ex. 1006, “Stefik”).

II. ANALYSIS

For the reasons discussed below, we determine Petitioner has shown by a preponderance of the evidence that claims 9 and 29 are anticipated by Arnold and that claims 9 and 29 would have been obvious over Arnold. We, however, determine that Petitioner has not shown by a preponderance of the evidence that claims 9 and 29 would have been obvious over the combination of Chang and Stefik.

We start first with a summary of the relevant legal standards, then provide an analysis of the level of skill in the art and claim construction, and then analyze the parties' contentions with respect to each of the asserted grounds.

A. Legal Standards

"In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")); *see also* 37 C.F.R. § 42.104(b) (requiring a petition for *inter partes* review to identify how the challenged claim is to be construed and where each element of the claim is found in the prior art patents or printed publications relied upon).

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. Inc., v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987); *see also Finisar Corp. v. DirecTV Group, Inc.*, 523 F.3d 1323, 1334 (Fed. Cir. 2008) (To anticipate a patent claim under 35 U.S.C.

§ 102, “a single prior art reference must expressly or inherently disclose each claim limitation.”). Moreover, “[b]ecause the hallmark of anticipation is prior invention, the prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements ‘arranged as in the claim.’” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). This is not an *ipsissimis verbis* test, however—identical terminology is not required. *See In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990). Whether a reference anticipates is assessed from the perspective of an ordinarily skilled artisan. *See Dayco Prods., Inc. v. Total Containment, Inc.*, 329 F.3d 1358, 1368 (Fed. Cir. 2003) (“[T]he dispositive question regarding anticipation [i]s whether *one skilled in the art* would reasonably understand or infer from the [prior art reference’s] teaching that every claim element was disclosed in that single reference.”). Additionally, under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates. *MEHL/Biophile Int’l Corp. v. Milgraum*, 192 F.3d 1362, 1365 (Fed. Cir. 1999); *In re Cruciferous Sprout Litig.*, 301 F.3d 1343, 1349–50 (Fed. Cir. 2002).

A claim is unpatentable under 35 U.S.C. § 103(a) if “the differences between the subject matter sought to be patented 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.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art;

(3) the level of skill in the art; and (4) when in evidence, objective evidence of obviousness or nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2016) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)). Furthermore, Petitioner does not satisfy its burden of proving obviousness by employing “mere conclusory statements,” but “must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

B. Level of Ordinary Skill in the Art

Petitioner contends that a person of ordinary skill in the art (a “POSITA”) at the time the ’721 patent was made would have had a minimum of a Bachelor of Science degree in computer science, electrical engineering, or a related field, and approximately one year of professional experience or equivalent study in distributed computing systems, including securing those systems. Pet. 17. Petitioner further states that additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. *Id.* at 17–18 (citing Ex. 1002 ¶¶ 33–34).

Patent Owner sets forth a similar definition, stating that a POSITA at the time the ’721 patent was filed would have had a Bachelor of Science degree in electrical engineering and/or computer science, and three years of

work or research experience in the fields of secure transactions and encryption, or a Master's degree in electrical engineering and/or computer science and two years of work or research experience in related fields. PO Resp. 19. Patent Owner states that the positions set forth in its Response would be the same under either party's proposal. *Id.*

The parties' proposals do not differ in any meaningful way to the issues in dispute. We adopt Petitioner's articulation of the level of ordinary skill in the art, except that we delete the qualifier "a minimum" to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an upper bound, i.e., encompassing a Ph.D. degree and beyond, and thus does not meaningfully indicate the level of ordinary skill in the art. This definition of a POSITA is supported by the testimony of Dr. Chatterjee and is commensurate with the level of ordinary skill as reflected in the prior art and the '721 patent. We note, however, that our analysis would be the same under either party's definition of a POSITA.

C. Claim Construction

In *inter partes* reviews, we interpret a claim "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b)." *See* 37 C.F.R. § 42.100(b). Under this standard, we construe the claim "in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." *Id.* Only claim terms that are in controversy need to be construed and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

1. “load module”

Petitioner argues the term “load module” recited in claim 9 should be construed as “executable code, such as a computer program or an applet, plus any associated data required for code execution.” Pet. 19. To support this proposed construction, Petitioner cites the Specification’s statements that “[l]oad modules may contain algorithms, data, cryptographic keys, shared secrets, and/or other information that permits a load module to interact with other system components,” and “[f]or a load module to operate and interact as intended, it must execute without unauthorized modification.” *Id.* (emphasis omitted) (quoting Ex. 1001, 3:28–35); *see also id.* at 19–20 (citing Ex. 1001, 4:36, 4:51–56, 5:34–39). Petitioner also points to the “Field of the Invention” section of the ’721 patent, which provides that “[t]he present invention relates to . . . techniques for certifying load modules such as executable computer programs or fragments [(called ‘applets’)] thereof as being authorized for use by a protected or secure processing environment.” *Id.* at 20 (alterations in original) (emphasis omitted) (quoting Ex. 1001, 1:17–28) (citing Ex. 1001, 2:33–37; Ex. 1002 ¶¶ 67–69).

According to Patent Owner, Petitioner’s proposed construction is inconsistent with the construction adopted in co-pending litigation of the related matters, in which the term was construed to mean “executable code and any associated data.” PO Resp. 22 (citing Ex. 2007, 44). Nevertheless, Patent Owner contends that the term “load module” does not require construction and should be given its plain and ordinary meaning. *Id.* Patent Owner further asserts that construction of this term is not necessary to resolve the matters presently in dispute and that its arguments would apply equally under the construction of the co-pending litigation or under a plain and ordinary meaning of the term. *Id.*

Based on the arguments presented by the parties and the issues raised, we agree with Patent Owner that no explicit construction of this phrase is necessary to resolve the disputes between the parties.

2. *“associated digital signature”*

Patent Owner points out that “the District Court [for the Eastern District of Texas] adopted a construction of ‘associated digital signature’ as ‘a digital value, verifiable with a public key, that can be used to determine the source and integrity of the load module/executable.’” PO Resp. 21 (citing Ex. 2001, 1). Nevertheless, Patent Owner contends that the term “associated digital signature” does not require construction and that its arguments would apply equally under the District Court’s construction or a plain and ordinary meaning of the term. *Id.* at 23. Petitioner does not provide its own construction of the term “associated digital signature.”

Based on the arguments presented by the parties, we agree with Patent Owner that no explicit construction of this term is necessary to resolve the disputes between the parties.

3. *Whether limitations (c) and (d) are conditional*

Claim 9 recites:

(c) if the load module has an associated digital signature, authenticating the digital signature using at least one public key secured behind a tamper resistant barrier and therefore hidden from the user; and

(d) conditionally executing the load module based at least in part on the results of authenticating step (c).

Ex. 1001, 22:10–16. Claim 29 recites similar limitations. *Id.* at 24:16–22.

In its Reply Brief, Petitioner contends that limitations (c) and (d) of claim 9, and the corresponding limitations of claim 29, are contingent steps that should not be given patentable weight. Pet. Reply 4–5. Specifically,

Petitioner argues that steps (c) and (d) “are only performed ‘**if the load module has an associated digital signature.**’” *Id.* According to Petitioner, the methods of claims 9 and 29 can be achieved by performing only steps (a) and (b). *Id.* at 5. Because only the first two steps are required to be performed, Petitioner argues the Board need not reach the optional method steps. *Id.* (citing *Ex parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 at *4 (PTAB, Apr. 28, 2016) (precedential)).

Patent Owner contends that Petitioner’s argument is a new argument, never raised in the Petition, and therefore should not be considered. PO Sur-reply 2–3. Patent Owner further argues that the claimed methods would be incomplete without limitations (c) and (d) which are necessary to distinguish between trusted and untrusted load modules and thus those limitations must be given weight. *Id.* at 4–5.

We agree with Patent Owner that Petitioner’s argument that limitations (c) and (d) are conditional is a new argument improperly raised for the first time in the Reply Brief. Petitioner has the burden to demonstrate sufficiently in the Petition that the cited prior art renders the challenged claims unpatentable, including showing that the Petition’s contentions are supported by evidence. *See* 35 U.S.C. § 314(a); *see also Harmonic Inc.*, 815 F.3d at 1363 (Fed. Cir. 2016) (“In an IPR, the petitioner has the burden *from the onset* to show *with particularity* why the patent it challenges is unpatentable.” (emphases added) (citing 35 U.S.C. § 312(a)(3))); *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (requiring “*the initial petition* identify ‘*with particularity*’ the ‘evidence that supports the grounds for the challenge to each claim.’” (emphases added)). This burden includes setting forth in its Petition “[h]ow the challenged claim is to be construed.” 37 C.F.R. § 42.104(b)(3).

The Petition sets forth arguments as to why the cited prior art references teach limitations (c) and (d) but does not include arguments indicating that these limitations should not be given patentable weight. *See* Pet. 49–55, 56–57, 72–80. In light of the contentions set forth in the Petition, Patent Owner’s Response focuses on arguing why the cited prior art references do not teach or disclose these limitations. PO Resp. 21–42. We do not find anything in Patent Owner’s Response that opens the door to Petitioner’s new arguments. Thus, we do not find Petitioner’s new position on claim construction to be permissible reply material and we do not consider it in making our decision. 37 C.F.R. § 42.23(b) (2021) (“A reply may only respond to arguments raised in the . . . patent owner response, or decision on institution.”).

D. Overview of the Cited Prior Art References

1. Overview of Arnold

Arnold, titled “System and method for secure storage and distribution of data using digital signatures,” generally relates to “an apparatus and method for secure distribution of software, software updates, and configuration data.” Ex. 1004, code (54), 5:19–20. Arnold describes the use of cryptography to protect software or data updates sent to computer products or peripherals using non-secure distribution channels (*id.* at 5:20–21), including an embodiment using “only public key cryptography” (*see, e.g., id.* at 5:37–40, 6:9–36, Figs. 2–3) and an embodiment using both “public key and symmetric key cryptography” (*see, e.g., id.* at 5:41–44, 6:3–4, 6:38–7:5, Figs. 4–5).

Figure 1 of Arnold is reproduced below.

FIG. 1

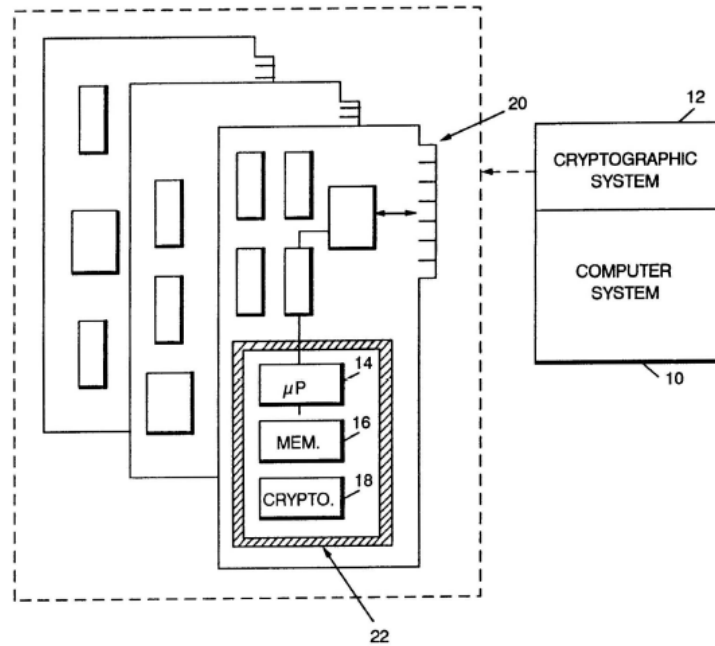


Figure 1 of Arnold is a block diagram depicting computer system 10 including “cryptographic system 12 comprising microprocessor 14, memory 16, and cryptographic functions 18 mounted upon . . . adapter card 20.” Ex. 1004, 5:35–36, 5:49–51. The microprocessor, memory, and cryptographic functions are housed within a secured area or module 22. *Id.* at 5:51. Public key KPU is installed in the adapter card 20. *Id.* at 5:52. Cryptographic system 12 includes the public key algorithm (e.g., RSA). *Id.* at 5:52–53.

Figure 2 of Arnold is reproduced below.

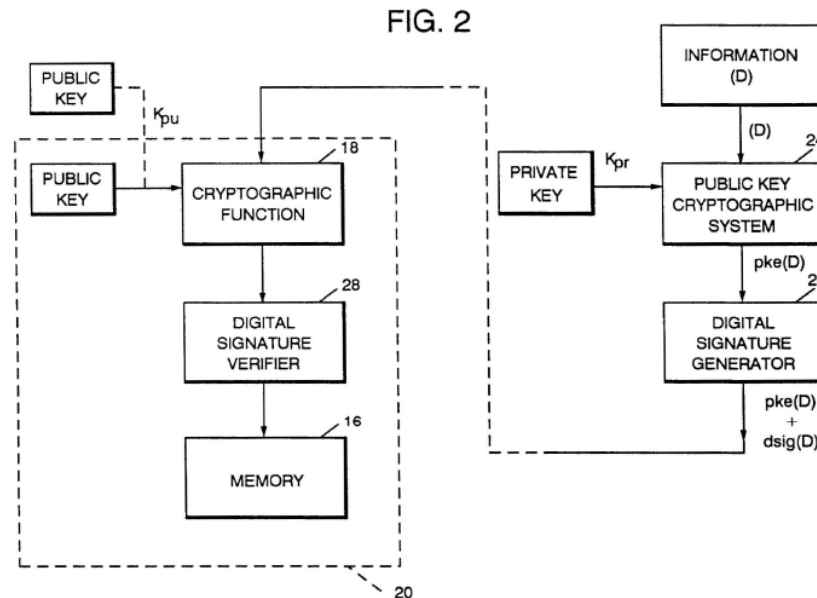


Figure 2 of Arnold is a block diagram of an embodiment employing public key cryptography for the secure distribution of software and data.

See Ex. 1004, 5:37–38; see also *id.* at 5:41–52 (stating Figure 4 depicts a block diagram of an embodiment employing both public key cryptography and symmetric key cryptography), Fig. 4. As shown in Figure 2, data (D) may be encrypted by public key cryptographic system 24 using private key KPR to generate pke(D). *Id.* at 5:56–58, Fig. 2; see also *id.* at Fig. 4 (also depicting public key cryptographic system 24). A digital signature on data (D) called dsig(D) may also be computed using digital signature generator 26. *Id.* at 6:1–2, Figs. 2, 4. Encrypted data pke(D) and digital signature dsig(D) are sent to the user, who loads the data into the secured area of adapter card 20. *Id.* at 6:25–27; 6:49–52. In the embodiment using only public key cryptography, the adapter decrypts the data using public key KPU, recovering clear data (D) and verifies the digital signature. *Id.* at 6:28–29. In the embodiment using public key and symmetric key cryptography, public key KPU is used to decrypt the symmetric key using

the public key algorithm and the recovered symmetric key is used to decrypt the data using the symmetric key algorithm. *Id.* at 6:52–54; *see also id.* at 6:2–4 (stating “the digital signature is verified before the data is accepted by digital signature verifier 28, which can be a component of cryptographic function 18” and that, preferably, “cryptographic function 18 include both a public key cryptographic system 18a and a symmetric cryptographic system 18b”). A verified digital signature proves, *inter alia*, that the data has not been altered since its creation. *Id.* at 6:4–6.

Figure 3 of Arnold is reproduced below.

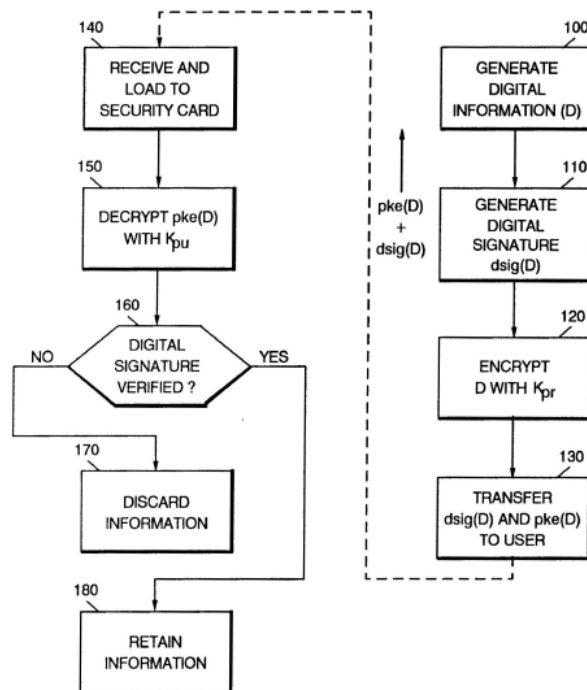


Figure 3 of Arnold depicts a flowchart of an embodiment employing public key cryptography for the secure distribution of software, software updates, and configuration data. Ex. 1004, 5:39–40; *see also id.* at 6:9–36 (describing the embodiment shown in Figure 3).

As shown in Figure 3, the manufacturer generates data (D) to be loaded into an adapter card and computes a digital signature (dsig(D)) on

data (D) using private key KPR (steps 100, 110). Ex. 1004, 6:13, 6:18–20. The manufacturer already possesses private key KPR, and the corresponding public key (public key KPU) may be embedded in the adapter card or supplied externally. *Id.* at 6:14–16. According to Arnold, public key KPU does not need to be kept secret in order to maintain integrity of the loaded data. *Id.* at 6:16–17; *see also id.* at 6:33–34 (“Only the private key KPR needs to be kept secret. The public key KPU is present in every copy of the device, and there is no security exposure if its value is divulged.”). Data (D) may be encrypted using a private key algorithm with private key KPR, yielding $pke(D)$ (step 120). *Id.* at 6:22–24. The manufacturer may send encrypted data $pke(D)$ and digital signature $dsig(D)$ to the adapter card user (step 130), who may receive this information and load it into the secured area of the adapter card (step 140). *Id.* at 6:25–27. The adapter card may then decrypt encrypted data $pke(D)$ using public key KPU and recover clear data D (step 150). *Id.* at 6:28. Digital signature $dsig(D)$ may be verified using the same key (step 160). *Id.* at 6:28–29. Once data $pke(D)$ has been decrypted and signature $dsig(D)$ has been verified, clear data (D) may be applied to the nonvolatile memory in the adapter card (step 180) or otherwise discarded (step 170). *Id.* at 6:30–32.

Figure 5 of Arnold is reproduced below.

FIG. 5

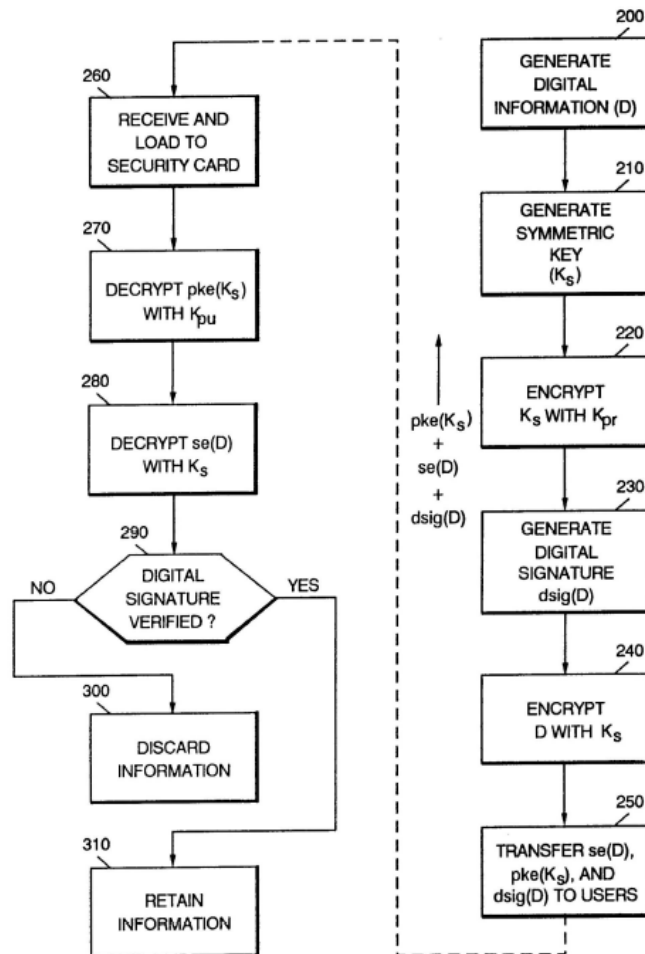


Figure 5 of Arnold depicts a flowchart of an embodiment employing both public key cryptography and symmetric key cryptography. Ex. 1004, 5:43–44; *see also id.* at 6:38–7:5 (describing the embodiment shown in Figure 5). In step 260 of Figure 5, encrypted data (including encrypted data pke(D), encrypted digital signature dsig(D), and an encrypted random symmetric algorithm key) is received at the user site where the adapter cards are installed and the data is loaded into the “secured area of the card, which contains . . . public key KPU.” *Id.* at 6:44–52. The public key is used to decrypt the symmetric key and the recovered symmetric key is used to

decrypt the data using the symmetric key algorithm (steps 270, 280). *Id.* at 6:51–54. The digital signature is verified using KPU (step 290). *Id.* at 6:55. If the signature verifies, then both data D and key KS (the random symmetric algorithm key) were valid and the data is loaded into the adapter card and enabled for use. *Id.* at 6:55–57. All cryptographic calculations are preferably performed inside the secured area of the adapter card so there is no threat of data manipulation while the data is recovered and verified. *Id.* at 6:57–59.

Arnold also describes, in its “Description of Related Art” section, “the IBM 4755 Cryptographic Adapter” as “a device which includes a microprocessor, memory, and programming logic mounted on a printed circuit board” with “[f]unctions . . . housed within a tamper-resistant module, or secured area, for protection.” Ex. 1004, 4:18–21.

2. *Overview of Chang*

Chang, titled “Method and Apparatus for Enhancing Software Security and Distributing Software,” generally relates to using public key encryption techniques for achieving enhanced security and product authentication in the distribution of software. Ex. 1005, code (54), 1:6–11, 3:15–17. Chang describes the problem of “authenticating that [the] software distributed by a manufacturer is a legitimate copy of an authorized software release, and that the software contains only the original manufacturer’s code without tampering.” *Id.* at 3:2–5. To address this problem, Chang describes using a “software passport,” which includes the digital signature of the application writer and manufacturer. *Id.* at 3:7–8. Chang describes that “[t]he software passport provides the basis of a trust model and allows

computer users to identify and determine the genuineness of a software product based on the information contained in its passport.” *Id.* at 6:34–38.

Figure 3 of Chang is reproduced below.

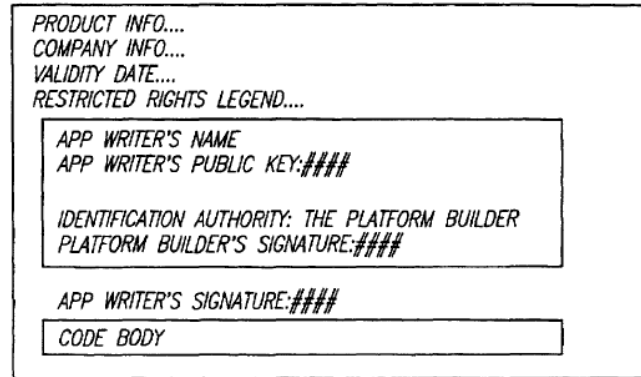
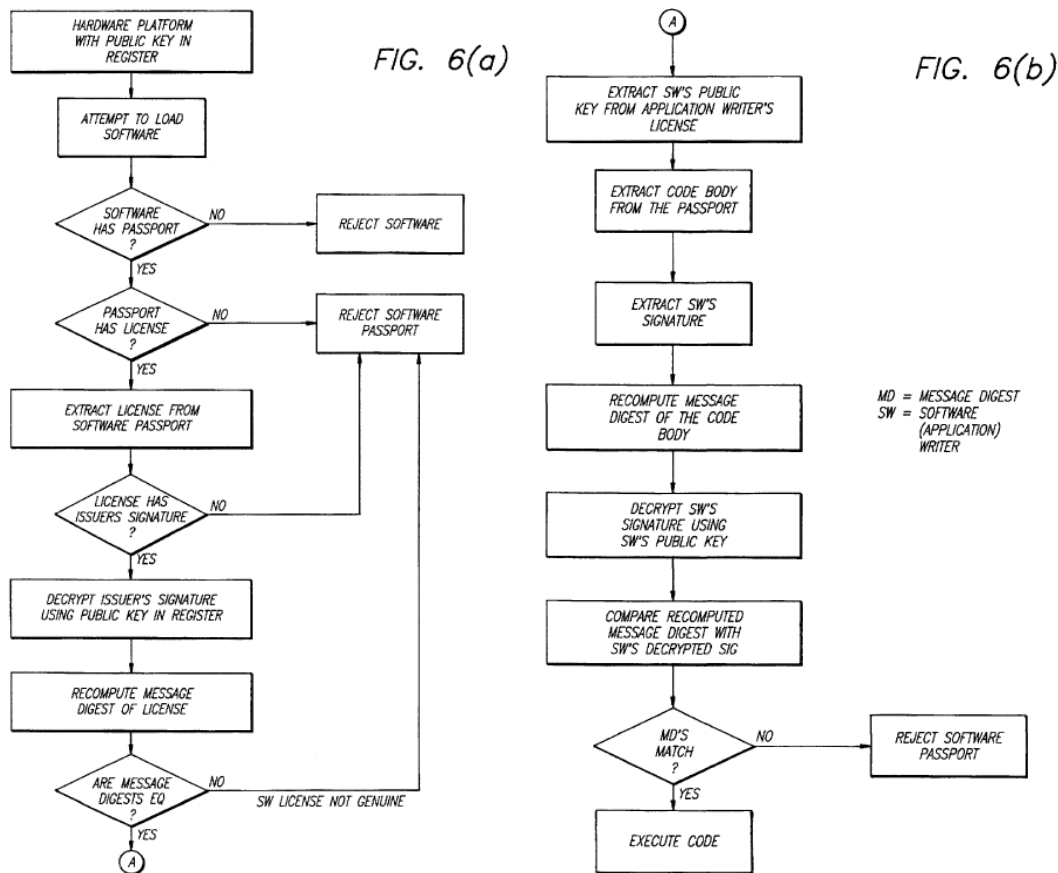


FIG. 3

Figure 3 of Chang depicts a software passport. Ex. 1005, 4:51–54, 6:42–45. As shown in Figure 3, the software passport may include, among other things, the application writer’s public key, the software code body including executable application code distributed to the user an application writer’s license, and the platform builder’s digital signature. *Id.* at 6:48–63, Fig. 3.

Figures 6a and 6b of Chang are reproduced below.



Figures 6a and 6b of Chang are flowcharts for verifying that a valid software license exists, and that the application writer's digital signature is valid, prior to permitting execution of a computer program. Ex. 1005, 4:59–63. As shown in Figure 6a, after determining that the software has a passport and an application writer's license, the platform may extract the public key embedded in the platform to verify that the passport's license is valid. *Id.* at 9:27–31. The license validation process may be accomplished by recomputing the message digest of the application license in the passport, recovering the original message digest (by decrypting the issuer's (platform builder's) digital signature using the platform builder's public key), and comparing the old digest with the newly computed digest. *Id.* at 9:34–43.

The system determines that the passport contains a valid application writer's license if the two message digests are the same. *Id.* at 9:44–45.

As shown in Figure 6b, the system also may verify that the application writer's digital signature is valid. Ex. 1005, 9:53–55. The signature validation process may be accomplished by recomputing the message digest of the passport, recovering the original message digest (by decrypting the application writer's digital signature using the application writer's public key embedded in the application writer's license within the passport), and comparing the old digest with the newly computed digest. *Id.* at 9:59–67. The system determines that the signature is valid if the two message digests are the same. *Id.* at 10:1–2. After verifying that the license and signature are valid, the operating system (OS) may obtain an additional approval to run the code, and the code may be executed. *Id.* at 10:15–22, Fig. 6b; *see also id.* at 4:29–40.

Figure 5 of Chang is reproduced below.

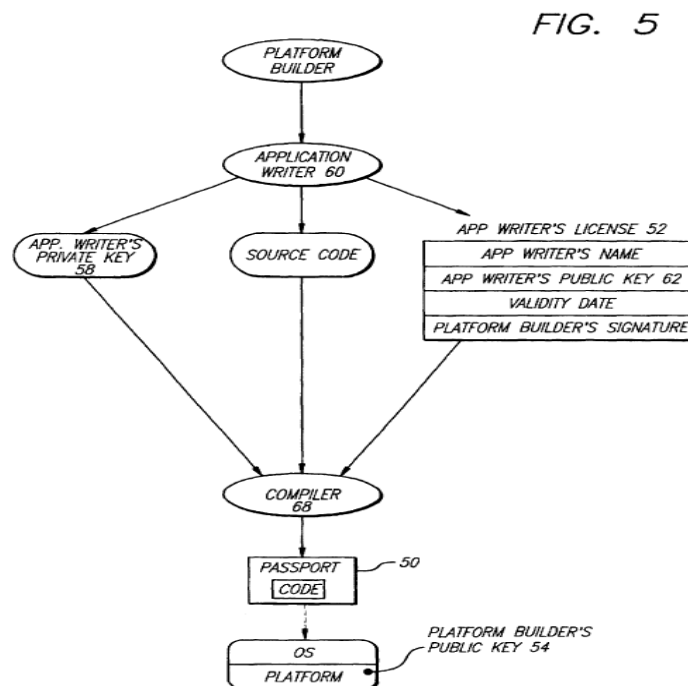


Figure 5 of Chang depicts the components of software passport 50 being issued by the platform builder, compiled by compiler 68, and then provided to (and received by) an end user of the OS running on the platform.

Ex. 1005, 4:57–58, 8:55–65, 9:19–23, 10:10–11, Fig. 5; *see also id.* at 8:25–32, 8:49–54, Fig. 4. The end user may be provided both the application writer’s public key 62 as well as the platform builder’s public key 54. *Id.* at 9:27–28, 9:59–61.

3. Overview of Stefik

Stefik, titled “System for Controlling the Distribution and Use of Digital Works Having Attached Usage Rights Where the Usage Rights Are Defined by a Usage Rights Grammar,” generally relates to controlling the use and distribution of digital works, such as software. Ex. 1006, code (54), 4:4–8. Stefik describes a system in which digital works and their attached usage rights are stored in and transmitted between repositories. *Id.* at 4:40–42.

Figure 2 of Stefik is reproduced below.

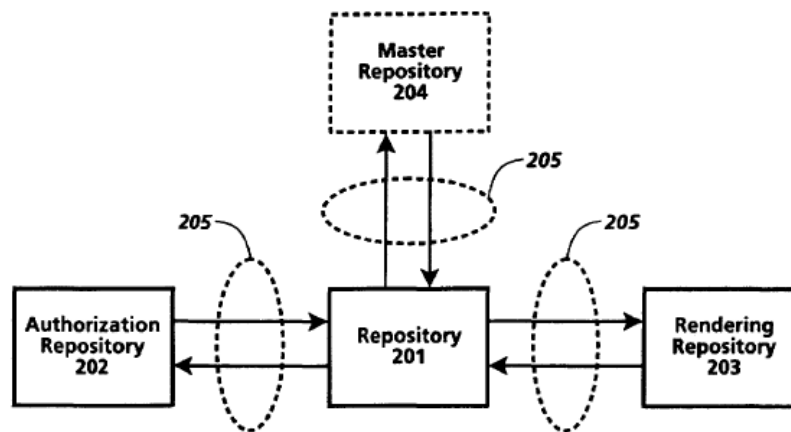


Fig. 2

Figure 2 of Stefik is a block diagram depicting various repository types and the repository transaction flow between them. Ex. 1006, 4:55–58, 7:49–50.

The various repository types serve different functions but share a core set of functionality enabling secure and trusted communications. *Id.* at 7:50–54. As shown in Figure 2, repository 201, a general instance of a repository, receives and processes access requests to digital works while in server mode, and initiates requests to access digital works while in requester mode. *Id.* at 7:54–60. Repository 201 may communicate via repository transaction protocol 205 with a plurality of other repositories, including authorization repository 202, rendering repository 203, and master repository 204. *Id.* at 7:62–67. Communication with authorization repository 202 may occur when a digital work being accessed has a condition that needs authorization. *Id.* at 8:1–3. Communication with rendering repository 203 may occur in connection with rendering a digital work. *Id.* at 8:10–11. And communication with master repository 205 may occur in connection with obtaining an identification certificate, by which a repository is identified as “trustworthy.” *Id.* at 8:15–18.

Stefik describes the use of public keys by the master repository and rendering repository as follows:

Key management and security is instrumental in the success of a public key encryption system. In the currently preferred embodiment, one or more master repositories maintain the keys and create the identification certificates used by the repositories.

Ex. 1006, 27:11–15.

[T]he master repository has special functionality for issuing digital certificates and maintaining encryption keys.

Id. at 15:25–27.

The requester [(rendering repository)] decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for

decrypting the software, the compatibility information, and a tamper-checking code. (This step certifies the software.).

Id. at 42:48–53; *see also id.* at 43:32–34.

Stefik further describes that a repository may be embedded in a device or enclosed in a secure housing as follows:

[T]he repository could be embedded in a “card” that is inserted into an available slot in a computer system.

Id. at 16:59–61.

The hardware embodiment of a repository will be enclosed in a secure housing which if compromised, may cause the repository to be disabled.

Id. at 14:16–19, Fig. 12.

Stefik also describes repository security levels including level 4 and above at which “[s]ensors are used to record attempts at physical and electronic tampering” and, “[a]fter such tampering, the repository will not perform other transactions until it has reported such tampering to a designated server.” Ex. 1006, 16:21–38; *see also id.* at 8:43–50 (describing that communications within a printer system and its printer repository are assumed to be secure), 9:11–13 (describing a computer system having a security boundary within which communications are assumed to be secure).

E. Anticipation by Arnold

Petitioner contends claims 9 and 29 are anticipated by Arnold. Pet. 39–57. As explained above, claims 9 and 29 are independent and recite similar limitations, with the only difference being that claim 9 recites “load modules” whereas claim 29 recites “executables.” Ex. 1001, 22:5–15, 24:10–21. Because of their similarities, Petitioner provides nearly identical contentions for both these claims (*compare* Pet. 43–55, *with* Pet. 56–57) and Patent Owner’s arguments also equally apply to both these claims (PO Resp.

21–31). In the sections below we analyze Petitioner’s contentions with respect to claim 9 but our analysis also equally applies to claim 29, as does our conclusion.

1. Preamble and Limitations (a) and (b)

Claim 9 recites “A method of distinguishing between trusted and untrusted load modules comprising: (a) receiving a load module, (b) determining whether the load module has an associated digital signature.” Ex. 1001, 22:5–9. Petitioner contends Arnold discloses the preamble and limitations (a) and (b) of claim 9. Pet. 43–49. Patent Owner does not separately dispute Petitioner’s contentions. We analyze Petitioner’s contentions here.

Petitioner contends Arnold teaches a method of distinguishing trusted and untrusted load modules by disclosing a method for secure distribution of software, software updates, and configuration data. Pet. 43 (citing Arnold (57), 2:15–17). Petitioner identifies the software, software updates, and configuration data as the recited “load modules” because the software, software updates, and configuration data would be “executed immediately after the data is loaded.” *Id.* (citing Ex. 1004, 10:37–38). Arnold distinguishes between trusted and untrusted load modules, according to Petitioner, because it verifies a digital signature on the data (i.e. the software etc.) to verify the data is genuine and comes from a valid source. *Id.* at 43–44 (citing Ex. 1004, 5:14, 6:28–32, 6:55–57, Fig. 3; Ex. 1002 ¶¶ 130–133, 162).

Petitioner contends that as part of the process of distributing data (software, software updates, etc.) to the user, Arnold computes a digital signature on the data and sends the signature along with the data to the

receiving device, which verifies the signature before the data is accepted. Pet. 47–49 (citing Ex. 1004, 2:5–17, 5:12–25, 5:52–59, 6:1–6, 6:13–32, 9:56–10:38, Figs. 2, 3; Ex. 1002 ¶¶ 134–138, 140, 162). Thus, Petitioner contends Arnold discloses “receiving a load module” and “determining whether the load module has an associated digital signature.”

We are persuaded by Petitioner’s contentions. Generally, a preamble does not limit a claim. *Allen Eng’g Corp. v. Bartell Indus., Inc.*, 299 F.3d 1336, 1346 (Fed. Cir. 2002). Here, we need not decide whether the preamble limits claim 9 because Petitioner establishes that Arnold teaches the preamble of claim 9. Arnold discloses a system and method for the secure distribution of software. Ex. 1004, code (57). To provide the required security, Arnold encrypts the software and generates a digital signature for the software. Ex. 1004, 6:44–59. The encrypted software and the digital signature are then sent to the user. *Id.* When the software is received, its digital signature is verified in order verify the origin of the data. *Id.* If the signature verifies, the software is loaded into the memory of the receiving device. *Id.* Dr. Chatterjee provides credible testimony that, because Arnold verifies the digital signature before loading the software, Arnold teaches a method of distinguishing between trusted and untrusted load modules. Ex. 1002 ¶¶ 130–133. This evidence sufficiently supports Petitioner’s contentions regarding the preamble and limitations (a) and (b) of claim 9.

2. Limitation (c)

Limitation (c) of claim 9 recites “if the load module has an associated digital signature, authenticating the digital signature using at least one public

key secured behind a tamper resistant barrier and therefore hidden from the user.” Ex. 1001, 22:10–13.

Petitioner contends that Arnold discloses a security adapter card with a secure area and that this secure area is a “tamper resistant barrier” as recited in claim 9. Pet. 49–50 (citing Ex. 1004, 5:9–13, 10:47–48; Ex. 1002 ¶ 143). Petitioner contends that Arnold discloses that, when the user receives the encrypted software and digital signature, it “loads the data and signature into the secured area of the adapter card.” *Id.* at 49 (quoting Ex. 1004, 6:26–27). Petitioner further contends that Arnold’s public key is used to verify the digital signature of Arnold’s load modules and that this public key is contained in the secure area of the adapter card. *Id.* at 49–53 (citing Ex. 1004, 3:56–57, 5:9–13, 5:52–53, 6:28–30, 6:51–59; Ex. 1002 ¶¶ 141–144, 162). Thus, Petitioner contends Arnold discloses authenticating the digital signature using at least one public key secured behind a tamper resistant barrier and, therefore, hidden from the user as recited in limitation (c).

Patent Owner contends that Arnold does not disclose that the public key is hidden from the user, which Patent Owner interprets as requiring that the public key have no read access. PO Resp. 21–28. Patent Owner makes two primary arguments in this regard. First, Patent Owner argues the public key in Arnold, in contrast to a private key, is described as not being kept secret and, therefore, not hidden from the user. *Id.* at 23 (citing Ex. 1003, 6:15–17, 6:33–34, Ex. 2027 ¶¶ 67–69). Second, Patent Owner argues that the public key is not kept in the secured area of the adapter card and, therefore, not secured behind a tamper resistant barrier and hidden from the user. *Id.* at 23–27 (citing Ex. 1004, Figs. 1, 2).

After considering the arguments and evidence presented by both parties, we are persuaded that Arnold discloses limitation (c) of claim 9. Arnold discloses an adapter card with a secured area. Ex. 1004, 5:49–51 (describing that the microprocessor, memory, and cryptographic functions of Arnold’s cryptographic system are “housed within a secured area or module” of an adapter card); Pet. 49–50. Arnold describes the secured area of its adapter card as an area “where data is protected from disclosure” (Ex. 1004, 5:10) and “which is protected from physical and direct electrical access” (Ex. 1004, 10:47–48). Pet. 49–50. These disclosures indicate that the secured area of Arnold’s adapter card is a “tamper resistant barrier” that prevents the data stored within from read access and, therefore, keeps the data “hidden from the user” as recited in limitation (c). We also credit Dr. Chatterjee’s testimony that, based on Arnold’s description of the secured area of the adapter card, the secured area forms a tamper resistant barrier that keeps data stored within, hidden from the user. Ex. 1002 ¶¶ 141–144 (citing Ex. 1004, 3:56–57, 5:9–12, 5:52–53, 6:13–32, 6:28–30, 6:51–52, 6:55–59).

Arnold makes clear that the “secured area of the card . . . contains the public key KPU” (Ex. 1004, 6:51–52) and that “said public key (K_{PU}) is stored within said secured area.” Ex. 1004, 12:25; *see also id.* at 12:42 (“means for providing a public key (K_{PU}) within said secure areas”); Pet. Reply 9. Dr. Chatterjee’s testimony, which we determine to be credible, also supports Petitioner’s contention that Arnold’s public key is within the secured area of Arnold’s adapter card. Ex. 1002 ¶ 143 (“The public key is secured behind a tamper resistant barrier and therefore hidden from the user.”).

The above disclosures indicate that (1) Arnold’s public key is stored in the secure area of Arnold’s adapter card and that (2) the secure area protects data from disclosure and prevents physical and direct electrical access.⁵ Thus, we agree with Petitioner that Arnold’s public key is “secured behind a tamper resistant barrier and therefore hidden from the user” as recited in claim 9.

Patent Owner argues that Arnold’s disclosures that the public key “does not need to be kept secret in order to maintain integrity of the loaded data” and that “[o]nly the private key KPR needs to be kept secret” indicate that the public key is not kept hidden from the user. PO Resp. 22–23 (citing Ex. 1004, 6:15–17, 6:33–34). Similarly, Patent Owner points to Figures 1 and 2 of Arnold to argue that these figures show the public key is not contained within the secure area of Arnold’s adapter card and therefore, not hidden from the user. PO Resp. 26. Figures 1 and 2 of Arnold, as annotated by Patent Owner, are reproduced below for convenience.

⁵ In Petitioner’s Reply Brief, Petitioner additionally relies on U.S. Patent No. 5,027,397 (“Double”) (Ex. 1015), which Petitioner argues Arnold incorporates by reference, as disclosing a tamper resistant barrier that prevents interrogation of data stored within and, therefore, keeps that data hidden from the user. Pet. Reply 6 (citing Ex. 1004, 4:18–21, 1015, 3:38–42). In reaching our conclusion that Arnold discloses limitation (c), we do not rely on Petitioner’s contentions regarding Double for the ground based on anticipation by Arnold.

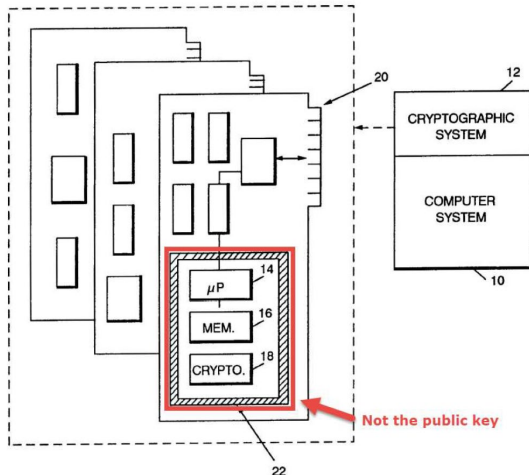


FIG. 1 (annotations added)

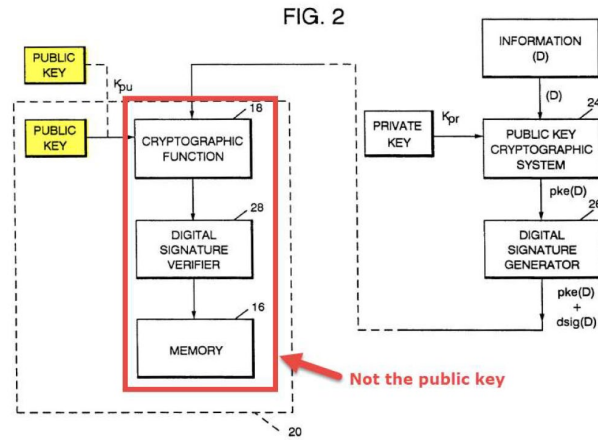


FIG. 2 (annotations added)

Id. at 25–26. Figure 1 of Arnold shown above, depicts Arnold’s computer system with its cryptographic system enlarged and broken out. Ex. 1004, 5:35–36. Patent Owner argues that Figure 1 does not show the public key as being contained in secured area 22 of Arnold’s adapter card 20. PO Resp. 25. Figure 2 of Arnold shown above, depicts a block diagram of an embodiment of Arnold’s system. Ex. 1004, 5:37–38. In Figure 2, public key K_{PU} is shown both inside and outside the dotted line representing Arnold’s secure card 20. Based on this depiction, Patent Owner argues the public key is “available to adapter card 20 from outside of the adapter card” and that Figure 2 “does not teach that the public key is restricted to the secure area 22 of adapter card 20, or being hidden from the user.” PO Resp. 26.

Based on the totality of the disclosure of Arnold, we disagree with Patent Owner’s arguments. Specifically, as explained above, Arnold is explicit in disclosing that the “secured area of the card . . . contains the public key K_{PU} ” (Ex. 1004, 6:51–52) and that “said public key (K_{PU}) is stored within said secured area.” Ex. 1004, 12:25; *see also id.* at 12:42 (“means for providing a public key (K_{PU}) within said secure areas”).

We agree with Petitioner that Arnold's disclosure that the public key does not need to be kept secret or that only the private key needs to be kept secret (Ex. 1004, 6:15–17, 6:33–34) describes the general nature of public and private keys but does not describe the more specific embodiments disclosed in Arnold where the public key is expressly described as being within the secured area of the adapter card. Pet. Reply 7–8. In other words, we determine that the express disclosure that the secured area contains the public key and that the public key is stored within said secured area more specifically describes Arnold's relied upon embodiments. The general description of public keys in Arnold that Patent Owner points to do not undermine these express disclosures.

Patent Owner takes issue with Arnold's express disclosure that "said public key (K_{PU}) is stored within said secured area" found in dependent claim 6 of Arnold because, as Patent Owner argues, it "only describes storing a public key in secure memory to *decrypt* encrypted data . . . not to authenticate a digital signature." PO Sur-reply 12. First, this argument does not account for the description in Arnold that the "secured area of the card . . . contains the public key KPU" and that the KPU is used to verify the digital signature, which Petitioner also relies on to show that the public key is contained in the secure area of the adapter card. Pet. 52 (citing Ex. 1004, 6:51–59). Second, we disagree that Arnold's disclosure in dependent claim 6 is limited only to decrypting encrypted data and does not apply to authenticating a digital signature. Dependent claim 6 of Arnold depends from independent claim 1. Ex. 1004, 12:24–25. Claim 1 of Arnold is directed to "[a] method of transferring data into a secured area" which refers to Arnold's method for secure storage and distribution of data in general. *Id.* at 11:50–55. This method "us[es] digital signature[s]." *Id.* at code (54).

Moreover, every embodiment of Arnold uses digital signatures to verify the data being loaded. *See id.* at Figs. 2–5. Thus, we determine that the public key referred to in Arnold’s dependent claim 6 is not limited to decrypting the distributed data but is also applies to verification using digital signatures.

Patent Owner argues that Figure 1 does not show the public key to be contained within the secure area of the adapter card. PO Resp. 25. But Figure 1 does not show the public key at all, whether within or outside the secure area. As such, Figure 1 cannot be taken to indicate the location of the public key one way or another. Figure 2 is a flow diagram that indicates the public key can be provided from within or from outside the card. As with the general description of public keys, Figure 2 does not specifically describe the relied upon embodiments (e.g. the “public key and symmetric key cryptography” embodiment) of Arnold. We determine that, when taken in light of Arnold’s explicit disclosures that the public key is contained in the secure area of the adapter card, Figure 2 is best interpreted as showing that the public key is provided from within the card.

For the aforementioned reasons, we agree with Petitioner that Arnold discloses limitation (c) of claim 9.

3. *Limitation (d)*

Limitation (d) recites “conditionally executing the load module based at least in part on the results of authenticating step (c).” Ex. 1001, 22:14–15. Petitioner relies on various passages from Arnold that indicate that Arnold’s data (e.g. software) is loaded if the associated signature is verified. Pet. 53–55 (citing Ex. 1004, 6:28–32, 6:55–59, 9:57–10:25, 10:37–38, 11:16; Ex. 1002 ¶¶ 146–149). Patent Owner does not separately dispute Petitioner’s contentions with regard to limitation (d).

We are persuaded by Petitioner’s arguments that Arnold discloses limitation (d). For example, Arnold discloses that, “[i]f the signature verifies, the data is genuine and it can only have been created by the manufacturer, who holds the private key KPR. Once the data has been decrypted and its validity has been determined, the data is applied to the nonvolatile memory in the adapter card, step 180; otherwise, the information is discarded, step 170.” Ex. 1004, 6:28–32. Arnold further discloses that, “[i]f the signature verifies, . . . the data is loaded into the nonvolatile memory on the adapter card and enabled for use, step 310.” *Id.* at 6:55–59.

For the reasons provided by Petitioner in its Petition (Pet. 53–55), we are persuaded Arnold discloses limitation (d).

4. Conclusion as to Anticipation over Arnold

For the reasons explained above, we determine that Petitioner has shown that Arnold discloses each limitation of claim 9 and claim 29 of the ’721 patent. Accordingly, we conclude that Petitioner has shown by a preponderance of the evidence the unpatentability of claims 9 and 29 as anticipated by Arnold.

F. Obviousness over Arnold

As explained above, Petitioner contends that Arnold anticipates claims 9 and 29, but nevertheless presents an alternative ground, arguing that even if Arnold does not explicitly meet limitation (c) (“a tamper resistant barrier and therefore hidden from the user”), a POSITA would have been motivated to apply the teachings of the related prior art disclosed in Arnold, including Double, to the secured area of Arnold’s adapter card so that this secured area would be tamper resistant and would keep the data stored within, “hidden from the user.” Pet. 57–59. Petitioner argues that Arnold

“expressly provides, it was well-known and desirable to house cryptographic functions, including keys, within a tamper-resistant module.” Pet. 58 (citing Ex. 1004, 4:16–21, 3:21–24). According to Petitioner, such a tamper-resistant module is disclosed in Double, which is incorporated by reference in Arnold. *Id.* (citing Ex. 1004, 4:16–21; Ex. 1015, 3:38–42; Ex. 1002 ¶¶ 164–165).

As before, Patent Owner argues that Arnold’s public key is described as being public and not hidden from the user, and that Arnold’s discussions of securing the key in tamper-resistant modules apply only to private keys. PO Resp. 28–29 (citing Ex. 2027 ¶¶ 83–85); PO Sur-reply 11. Thus, according to Patent Owner, these portions of Arnold cannot be used as motivation to combine with the other cited references to provide a tamper resistant barrier that keeps the public key hidden from the user. PO Resp. 30. With respect to the embodiment in which Arnold explicitly discloses that the “secured area of the card . . . contains the public key KPU,” Patent Owner argues that this embodiment does not disclose securing the public key at all times, but rather is more concerned with keeping the private key KS secret. *Id.* at 30–31 (citing Ex. 2027 ¶¶ 91–93).

Having considered the arguments and evidence presented by both parties, we are persuaded by Petitioner that Arnold along with its incorporated prior art, Double, teach limitation (c) of claim 9.⁶ Double discloses key store 14 that stores encryption keys, and a scheme for detecting and “preventing unauthorized interrogation” of the stored encryption keys in the key store. Ex. 1015, 3:38–42. We agree with

⁶ As explained above, we have already determined that Arnold discloses the preamble and limitations (a) (b) and (d) of claim 9. *See supra* Section II.E.1 and 3.

Petitioner that, by preventing interrogation of stored keys, Double teaches a tamper-resistant barrier that prevents read access and, therefore, keeps keys hidden from the user. When the teachings of Double's key store 14 are applied to the secured area of Arnold's adapter card 20, which Arnold discloses as containing and storing the public key, we agree with Petitioner that Arnold, and the incorporated disclosure of Double, teach a "public key secured behind a tamper resistant barrier and therefore hidden from the user."

We disagree with Patent Owner's argument that Arnold's discussion of the desirability of a tamper-resistant barrier (Ex. 1004, 4:18–21) and its discussion of keeping cryptographic functions and data secure (Ex. 1004, 3:21–24) would not apply to Arnold's public key. As explained above in our analysis of anticipation by Arnold, Arnold explicitly discloses that the public key is contained and stored within the secured area of its adapter card 20. *See supra* §§ II.E.2 (citing Ex. 1004, 1004, 6:51–52, 12:25, 12:42). Thus, a POSITA would have been motivated to secure the public key of Arnold just as they would have been motivated to secure other data stored in the secured area of Arnold's adapter card 20.

1. Objective Indicia of NonObviousness

In its Response, Patent Owner contends that there is evidence of long-felt need, failure of others, industry praise, commercial success, and copying which should be considered as objective indicia of nonobviousness. PO Resp. 42–45.

For us to give substantial weight to objective indicia of obviousness or nonobviousness, a proponent must establish a nexus between the evidence and the merits of the claimed invention. *ClassCo, Inc., v. Apple, Inc.*, 838

F.3d 1214, 1220 (Fed. Cir. 2016). “[T]here is no nexus unless the evidence presented is ‘reasonably commensurate with the scope of the claims.’” *Id.* (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)).

A patentee is entitled to a presumption of nexus “when the patentee shows that the asserted objective evidence is tied to a specific product and that product ‘embodies the claimed features, and is coextensive with them.’” *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). But as Petitioner correctly argues (Pet. Reply 23–25), a presumption of nexus is inappropriate here because Patent Owner does not provide an analysis demonstrating that its products are coextensive (or nearly coextensive) with the challenged claim. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020).

But even without the presumption, Patent Owner “is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the ‘direct result of the unique characteristics of the claimed invention.’” *Fox Factory*, 944 F.3d at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). Also, the nexus must be “to some aspect of the claim *not already in the prior art.*” *In re Kao*, 639 F.3d 1057, 1069 (Fed. Cir. 2011) (emphasis added). “Ultimately, the fact finder must weigh the [objective indicia] evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan.” *Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331–32 (Fed. Cir. 2016)).

As we discuss below, we find that Patent Owner has not shown a nexus between the claimed invention and long-felt need, failure of others, industry praise, commercial success, or copying. Moreover, in addition to

this proceeding, Patent Owner presents nearly the same arguments and evidence with respect to objective indicia of nonobviousness in at least four other proceedings involving different patents. *See Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00661, Paper 17 at 63–68 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00662, Paper 17 at 60–65 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00664, Paper 15 at 63–66 (PTAB Mar. 2, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00665, Paper 19 at 62–66 (PTAB June 16, 2021) (Patent Owner Response). Patent Owner, however, does not explain adequately how the same evidence of objective indicia of nonobviousness can be attributable to each particular claimed invention. *See Fox Factory*, 944 F.3d at 1378 (“The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features. In such situations, the patentee retains the burden of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention.” (citation omitted)).

a) Long-Felt Need and Failure of Others

In order to show a long-felt but unmet need for the claimed invention, the objective evidence must show that the need was a persistent one that was recognized by those of ordinary skill in the art at the time of the invention. *In re Gershon*, 372 F.2d 535, 538 (CCPA 1967). As evidence of long-felt need and failure of others, Patent Owner submits three articles from the *Wall Street Journal* which, according to Patent Owner, suggest a need for a way to distribute digital content in a secure manner that would “(1) ensure the

digital content would only be used in an authorized manner, (2) ensure that the digital content creator would be compensated for use of the digital content, and (3) allow for such distribution to client devices that were not under the control of the distributor.” PO Resp. 42–43 (citing Ex. 2030, 1; Ex. 2031, 1; Ex. 2032, 1). Patent Owner also submits another article from the *Wall Street Journal*, and an article from the *New York Times*, describing work by Xerox PARC, IBM, Microsoft, and other companies in the area of digital rights management. *Id.* at 43 (citing Ex. 2033, 3; Ex. 2034, 1).

Patent Owner contends that “most, if not all, systems developed by others were either not commercially successful, were not adopted by digital content industries, copied the claimed invention or have been licensed under the claimed invention.” PO Resp. 43. But Patent Owner does not cite any evidence supporting this argument.

We assign this evidence little weight, because Patent Owner has not identified anything in the cited articles that ascribes any long-felt need to the merits of the claimed invention of the ’721 patent, and has not pointed to any evidence that others had failed to achieve a solution to any technical problem for which the invention of ’721 patent is also a solution.

b) Significance Recognized by the Industry

As evidence of industry recognition, Patent Owner submits an article published in *Fortune*. PO Resp. 44 (citing Ex. 2035). Patent Owner argues that the article praises Patent Owner’s technology for “wrap[ping] the file in a secure digital container and tag[ging] it with rules describing how it could be used,” and where, “[t]o play or read the . . . file, recipients would need special software or hardware that could be trusted by the content originator to enforce the rules.” *Id.* (alterations and omission in original) (emphasis

omitted) (quoting Ex. 2035, 2). According to Patent Owner, “the use of special software or hardware to govern access to digital content is the thrust of the subject claims of the ’721 patent.” *Id.* (citing Ex. 1001, 4:61–7:28).

In its Reply, Petitioner contends the *Fortune* article merely provides a high level summary of Patent Owner’s technology. Pet. Reply 24.

Petitioner argues that the mention of a “‘secure digital container’ and ‘rules’ in the article has nothing to do with the subject matter in claims 9 and 29 that is directed to a method of ‘distinguishing between trusted and untrusted load modules.’” Pet. Reply 24 (citing Ex. 2035, 2).

We determine that the *Fortune* article fails to provide a nexus to the claimed invention. We agree with Petitioner that the *Fortune* article provides only a high level summary of Patent Owner’s technology and that the mention of a “secure digital container” and “rules” have a tenuous connection with the claimed subject matter of the ’721 patent, which does not mention a “secure digital container” or “rules” that apply to such a container.

Thus, we find that Patent Owner has not shown that there is a nexus between the evidence of industry recognition and the merits of the claimed invention. Absent a nexus, we assign little weight to the evidence of industry praise.

c) Commercial Success and Copying

As evidence of commercial success and copying, Patent Owner argues that over two dozen companies have licensed the claimed invention, and that Patent Owner “has received more than \$1 billion in patent licensing revenue in return for granting licensees the right to practice the claimed invention and [Patent Owner’s] remaining patent portfolio.” PO Resp. 45.

But Patent Owner does not cite any evidence to support its contention, such as the mentioned licenses themselves, or any testimony by someone who was familiar with the circumstances of the licenses to Patent Owner's portfolio. Absent such evidence, we cannot assess whether the licenses have any nexus to the limitations of the challenged claims. Thus, we assign little weight to Patent Owner unsupported arguments on commercial success and copying.

2. Conclusion as to Obviousness over Arnold

For the reasons explained above we give little weight to Patent Owner's evidence of nonobviousness. On the other hand, based on the arguments and evidence presented in the Petition, we determine that Petitioner has shown that Arnold along with Double, incorporated by reference in Arnold, teach the limitations of claims 9 and 29 of the '721 patent. Weighing all of the evidence of obviousness and nonobviousness, we conclude that Petitioner has shown by a preponderance of the evidence the unpatentability of claims 9 and 29 as obvious over Arnold.

G. Obviousness over Chang and Stefik

Petitioner contends the combination of Chang and Stefik teaches the limitations of claims 9 and 29. Pet. 59–80. As before, Petitioner's contentions regarding claims 9 and 29 are nearly identical (*compare* Pet. 65–79, *with* Pet. 79–80), as are Patent Owner's arguments against Petitioner's contentions for these two claims (PO Resp. 30–42).

1. Combination of Chang and Stefik

Petitioner relies on Chang to teach most of the limitations of claims 9 and 29, but relies on Stefik primarily to teach a public key stored behind a tamper resistant barrier (i.e. Stefik's master repository). Pet. 64, 75 (citing

Ex. 1006, 14:16–18, 27:11–15, 42:30–60). Petitioner argues that a POSITA would have been motivated to apply Stefik’s teaching of storing public keys behind a tamper resistant barrier in implementing Chang’s method of distributing software where a public key is stored on Chang’s hardware platform. *Id.* at 64. A POSITA would do so because a tamper resistant barrier would enhance security ensuring that the keys are safeguarded. *Id.* As support for its proposed motivation to combine, Petitioner relies on Stefik’s teaching that “[k]ey management and security is instrumental in the success of a public key encryption system.” *Id.* (quoting Ex. 1006, 27:11–15). According to Petitioner, combining Stefik’s tamper resistant barrier with Chang would further Chang’s goal of “allow[ing] only authorized code to be executed” on its platform. *Id.* (citing Ex. 1005, 8:55–59; Ex. 1002 ¶ 175).

Patent Owner argues that it would not have been obvious to combine Chang and Stefik. PO Resp. 34–42. Specifically, Patent Owner argues that Stefik involves “two-way communications” and, thus, it is important for Stefik to prevent access to keys by third parties. *Id.* at 34–35 (citing Ex. 1006, 27:2–28:7). Chang, on the other hand, involves only one-way communication from a software distributor to a user of the software (but not from the user to the software distributor); thus, according to Patent Owner, keeping the public key hidden would be of no benefit because there are no encrypted communications from the user to the software publisher. *Id.* at 35–36 (citing Ex. 2027 ¶¶ 105–112). Patent Owner also argues Stefik’s tamper resistant barrier does not keep keys hidden from the user and, thus, a POSITA would not have been motivated to combine Stefik with Chang for that purpose. *Id.* at 36–39 (citing Ex. 2027 ¶¶ 113–115). Furthermore, Patent Owner argues that Petitioner’s motivation of enhancing security is a

general motivation that does not provide a specific reason to combine Stefik with Chang in the way argued by Petitioner. *Id.* at 37. According to Patent Owner, Petitioner's allegations are conclusory and tainted by impermissible hindsight reconstruction. *Id.* at 38–42.

Petitioner responds that that alleged difference between one-way and two-way communications of Chang and Stefik, respectively, are irrelevant to their asserted obviousness ground, which only relies on Stefik's teaching of securing keys behind a tamper resistant barrier. Pet. Reply 18.

Additionally, Petitioner argues Chang's disclosure that platform producers often desire to allow only authorized code on their platform would have motivated a POSITA to secure Chang's public key behind a tamper resistant barrier "to prevent a user from replacing the key." *Id.* at 19 (citing Ex. 1005, 8:55–59).

Having considered the evidence and arguments from both parties, we do not agree with Petitioner that it would have been obvious to combine Stefik's tamper resistant barrier with Chang. Petitioner argues that a tamper resistant barrier would enhance security and would further Chang's goal of allowing only authorized code to be executed on its platform. Pet. 64 (citing Ex. 1005, 8:55–59; Ex. 1006, 27:11–15). We agree with Patent Owner that this reason to combine is too general and conclusory to explain how the specific modification of securing Chang's public keys behind a tamper resistant barrier would have provided a relevant benefit to the combination beyond Chang's own secure distribution system that provides security, without placing the public key behind a tamper resistant barrier.

We determine that such a generalized and conclusory reason for combining Chang and Stefik is insufficient. *Magnum*, 829 F.3d at 1380 ("To satisfy its burden of proving obviousness, a petitioner cannot employ mere conclusory

statements. The petitioner must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.”). Specifically, Chang discloses that platform producers desire to allow only authorized code to be executed on their platform. Ex. 1005, 8:55–59. This is done by identifying the software that will execute on their platform. *Id.* at 8:60–62. Chang provides a solution to this problem by using software passports that include digital signatures. *Id.* at 8:65–9:48. Chang’s solution involves using a public key which is not kept behind a tamper resistant barrier. *Id.* Thus, Petitioner’s proposed motivation to combine to “enhance security” (Pet. 64) and to allow only authorized code to be executed on a platform does not explain why the public key would have to be kept behind a tamper resistant barrier.

In response to the argument that its motivation is too conclusory, Petitioner further explains that its proposed motivation to combine (a platform producer’s desire to allow only authorized code on their platforms) would have motivated a POSITA to secure Chang’s public key behind a tamper resistant barrier to prevent a user from replacing the key. Pet. Reply 19 (citing Ex. 1005, 8:55–59). We agree with Patent Owner that this motivation suffers from hindsight bias as it is the same motivation disclosed in the ’721 patent itself for securing public keys behind a tamper resistant barrier. Ex. 1001, 14:23–28 (“In addition, maintaining the ‘public’ key within a tamper resistant environment forecloses the significant threat that the owner of protected processing environment 108 may himself attack the environment.”). Petitioner does not provide evidence that the motivation of preventing the user themselves from replacing the public key was a known problem in the industry or that it stems from either Chang or Stefik. Without such evidence, we conclude that Petitioner’s articulated reason for

combining Chang and Stefik is tainted by impermissible hindsight reconstruction. *Sci. Plastic Prod., Inc. v. Biotage AB*, 766 F.3d 1355, 1359 (Fed. Cir. 2014) (“The pertinence of the reference as a source of solution to the inventor’s problem must be recognizable with the foresight of a person of ordinary skill, not with the hindsight of the inventor’s successful achievement.”).

Because we determine Petitioner has not provided a sufficient motivation to combine Chang with Stefik we need not further analyze its contentions regarding how this proposed combination teaches all the limitations of claims 9 and 29.

2. *Conclusion as to Obviousness over Chang and Stefik*

For the reasons stated above, Petitioner’s arguments and evidence that a POSITA would have combined Chang and Stefik in the manner alleged by Petitioner are not sufficient to justify a conclusion of obviousness. Accordingly, we conclude Petitioner has not shown by a preponderance of the evidence that claims 9 and 29 would have been obvious over Chang and Stefik.

III. CONCLUSION⁷

Weighing all of the evidence of obviousness and nonobviousness together, including the content of the prior art, the differences between the

⁷ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner’s attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent

prior art teachings and the claim limitations, and the objective indicia of nonobviousness, we determine that Petitioner has shown by a preponderance of the evidence that claims 9 and 29 are anticipated by Arnold and also would have been obvious over Arnold. We, however, determine that Petitioner has not shown by a preponderance of the evidence that claims 9 and 29 would have been obvious over Chang and Stefik.

In summary:

Claims	35 U.S.C. §	Reference(s)/ Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
9, 29	102	Arnold	9, 29	
9, 29	103	Arnold	9, 29	
9, 29	103	Chang, Stefik		9, 29
Overall Outcome			9, 29	

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED claims 9 and 29 of the '721 patent are held to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, the parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. §§ 42.8(a)(3), (b)(2).

IPR2020-01123

Patent 6,157,721

FOR PETITIONER:

Scott A. McKeown

Mark Rowland

Keyna Chow

ROPES & GRAY LLP

scott.mckeown@ropesgray.com

mark.rowland@ropesgray.com

keyna.chow@ropesgray.com

Leslie Spencer

DESMARAIS LLP

lspencer@desmaraisllp.com

FOR PATENT OWNER:

Christopher A. Mathews

Razmig Messerian

Tigran Guledjian

Scott Florance

QUINN EMANUEL URQUHART & SULLIVAN LLP

chrismathews@quinnemanuel.com

razmesserian@quinnemanuel.com

tigranguledjian@quinnemanuel.com

scottflorance@quinnemanuel.com