UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

BLACKBERRY LTD.,
Patent Owner.

Case IPR2017-01619
Patent 8,489,868

PETITIONER'S NOTICE OF APPEAL

Director of the United States Patent and Trademark Office
c/o Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a), that Petitioner Google LLC ("Petitioner") appeals to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered on December 19, 2018 (Paper 31) (the "Final Written Decision") by the United States Patent and Trademark Office, Patent Trial and Appeal Board (the "Board"), and from all underlying orders, decisions, rulings, and opinions. A copy of the Final Written Decision is attached.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Petitioner indicates that the issues on appeal include, but are not limited to, the Board's ruling that Petitioner has not demonstrated, by a preponderance of the evidence, that claims 77, 79, 80, 82, 86, and 112 of U.S. Patent No. 8,489,868 ("the '868 patent") are unpatentable over the prior art, and any findings or determinations supporting or related to that ruling including, without limitation, the Board's construction and application of the

claim language, the Board's interpretation of the prior art, and the Board's interpretation of expert evidence.

Simultaneous with this submission, a copy of this Notice of Appeal is being filed with the Board. In addition, the Notice of Appeal and the required fee are

being filed electronically with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

Respectfully submitted this 20th day of February, 2019.

Respectfully submitted,

Dated: February 20, 2019

By: /Naveen Modi/

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for Petitioner

CERTIFICATE OF SERVICE

The undersigned certifies that, in addition to being filed electronically through Patent Trial and Appeal Board End to End (PTAB E2E), the original version of this Notice of Appeal was filed by overnight express delivery on February 20, 2019 with the Director of the United States Patent and Trademark Office, at the following address:

Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

The undersigned also certifies that a true and correct copy of this Notice of Appeal and the required fee were filed electronically via CM/ECF on February 20, 2019, with the Clerk of Court for the United States Court of Appeals for the Federal Circuit.

The undersigned also certifies that a true and correct copy of this Notice of Appeal was served on February 20, 2019, on counsel of record for Patent Owner BlackBerry Ltd. by electronic mail (by agreement of the parties) at the following address:

Ching-Lee Fukuda
SIDLEY AUSTIN LLP
787 Seventh Avenue
New York, NY 10019
clfukuda@sidley.com

Samuel A Dillon
Sharon Lee
SIDLEY AUSTIN LLP
1501 K. Street, N.W.
Washington, D.C. 20005
samuel.dillon@sidley.com
sharon.lee@sidley.com

Dated: February 20, 2019

By: /Naveen Modi/

Naveen Modi
Registration No. 46,224
Paul Hastings LLP
875 15th Street, N.W.
Washington, DC 20005
(202) 551-1700
naveenmodi@paulhastings.com

Counsel for Petitioner

Trials@uspto.gov
571-272-7822

Paper 31
Entered: December 19, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner

v.

BLACKBERRY LTD.,
Patent Owner.

Case IPR2017-01619
Patent 8,489,868 B2

Before SALLY C. MEDLEY, ROBERT J. WEINSCHENK, and AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

Google LLC ("Petitioner") filed a Petition (Paper 1, "Pet.") for *inter partes* review of claims 1, 13, 76–95, 98, 100, 104, 108, 112, 113, 137–139, and 142–144 of U.S. Patent No. 8,489,868 B2 (Ex. 1001, "the '868 patent"). The Petition asserted that these claims are unpatentable on the following grounds (*see* Pet. 2–3):

References	Basis	Challenged Claim(s)
Garst[1] and Gong[2]	§ 103(a)[3]	1, 13, 76, 78, 81, 84, 85, 87, 88, 90–93, 95, 98, 100, 104, 108, 112, 113, 137–39, and 142–44
Garst, Gong, and Davis[4]	§ 103(a)	77, 79, 80, and 82
Garst, Gong, and Chang[5]	§ 103(a)	83
Garst, Gong, and Sibert[6]	§ 103(a)	86
Garst, Gong, and Wong-Insley[7]	§ 103(a)	89
Garst, Gong, and Haddock[8]	§ 103(a)	94

[1] U.S. Patent No. 6,188,995 B1, Feb. 13, 2001 (Ex. 1012).

[2] Li Gong, *Inside Java™ 2 Platform Security* (1999) (Ex. 1016).

[3] Because the effective filing date of the '868 patent is earlier than March 16, 2013, the pre-AIA version of § 103 controls.

[4] U.S. Patent No. 5,844,986, Dec. 1, 1998 (Ex. 1013).

[5] U.S. Patent No. 5,724,425, Mar. 3, 1998 (Ex. 1014).

[6] U.S. Patent No. 7,243,236 B1, July 10, 2007 (Ex. 1015).

[7] U.S. Patent No. 6,131,166, Oct. 10, 2000 (Ex. 1017).

[8] U.S. Patent No. 5,657,378, Aug. 12, 1997 (Ex. 1018).

We instituted an *inter partes* review on all grounds raised in the Petition. *See* Paper 9 ("Inst. Dec.") at 21.

The briefing in this proceeding now includes the Petition, a Patent Owner Response (Paper 16, "PO Resp."), a Petitioner Reply (Paper 19, "Reply"), and a Patent Owner Sur-Reply (Paper 26, "Sur-Reply"). On September 17, 2018, we held an oral hearing, together with IPR2017-01620, a transcript of which is included in the record as Paper 30 ("Tr."). Petitioner relies on a declaration by Dr. Patrick D. McDaniel (Ex. 1002, "McDaniel Decl."); Patent Owner relies on a declaration of Dr. George T. Ligler (Ex. 2002, "Ligler Decl."). Both experts were deposed, and the deposition transcripts were made of record. *See* Ex. 2004 ("McDaniel Tr."); Ex. 1046 ("Ligler Tr."). Patent Owner filed evidentiary objections (Papers 11 and 21), but no motion to exclude.

We have jurisdiction under 35 U.S.C. § 6. Petitioner bears the burden of proving unpatentability of the challenged claims, and the burden of persuasion never shifts to Patent Owner. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). To prevail, Petitioner must prove unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d).

This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. On this record, we determine, for the reasons detailed below, that Petitioner has shown by a preponderance of the evidence that claims 1, 13, 76, 78, 81, 83–85, 87–95, 98, 100, 104, 108, 113, 137–39, and 142–44 of the '868 patent are unpatentable, but has not shown that claims 77, 79, 80, 82, 86, and 112 are unpatentable.

B. Related Proceedings

The ’868 patent was at issue in *BlackBerry Ltd. v. BLU Products, Inc.*, No. 1-16-cv-23535 (S.D. Fla.). Pet. 1. According to PACER, the case was dismissed on August 15, 2017.

Petitioner concurrently filed another petition, IPR2017-01620, for *inter partes* review of the ’868 patent based on different prior art. Pet. 1. The 1620 petition does not challenge claims 87, 108, 138, 143, and 144.

Patent Owner is presently prosecuting a continuation of the ’868 patent, U.S. Serial No. 13/413,173.

C. The ’868 Patent

The ’868 patent describes “a code signing system and method” said to be “particularly well suited for Java™ applications for mobile communication devices, such as Personal Digital Assistants, cellular telephones, and wireless two-way communication devices.” Ex. 1001, 1:20–24.

The patent explains that “[i]n a typical software code signing scheme, a digital signature is attached to a software application that identifies the software developer” and “[o]nce the software is downloaded by a user, the user typically must use his or her judgment to determine whether or not the software application is reliable, based solely on his or her knowledge of the software developer’s reputation.” *Id*. at 1:30–36. The patent identifies two drawbacks to this prior art scheme. First, it “does not ensure that a software application written by a third party for a mobile device will properly interact with the device’s native applications and other resources.” *Id.* at 1:37–43. Second, “[b]ecause typical code signing protocols are not secure and rely solely on the judgment of the user, there is a serious risk that destructive . . .

software applications may be downloaded and installed onto a mobile device." *Id.*

The solution described in the '868 patent is "[a] code signing system [that] operates in conjunction with a software application having a digital signature." *Id.* at 1:54–56. An application programming interface ("API") is "configured to link the software application with [an] application platform" and "[a] virtual machine verifies the authenticity of the digital signature in order to control access to the API by the software application." *Id.* at 1:58–61.

The main embodiment of the '868 patent is described with reference to Figure 1:

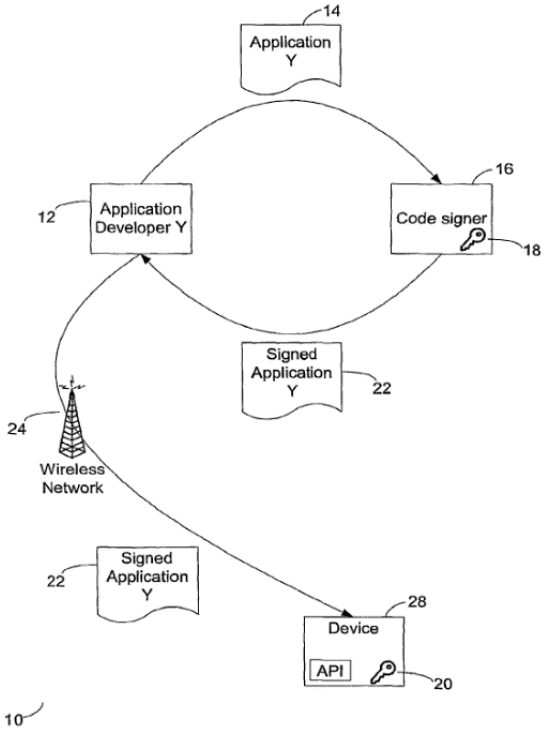

Figure 1

Figure 1 represents "a code signing protocol according to one embodiment of the invention." Ex. 1001, 2:54–55.

As illustrated, "[a]n application developer 12 creates a software application 14 (application Y) for a mobile device that requires access to one or more sensitive APIs on the mobile device." *Id.* at 3:9–12. Then, "[s]oftware application Y 14 is sent from the application developer 12 to the code signing authority 16." *Id.* at 4:24–26. "If the code signing authority 16 determines that software application Y 14 may access the sensitive API and therefore should be signed, then a signature . . . for the software application Y 14 is generated by the code signing authority 16 and appended to the software application Y 14." *Id.* at 4:36–40. "The signed software application Y 22 may then be sent to a mobile device 28 or downloaded by the mobile device 28 over a wireless network 24" and, "[o]nce the signed software application Y 22 is loaded on the mobile device 28, each digital signature is preferably verified with a public signature key 20 before the software application Y 14 is granted access to a sensitive API library." *Id.* at 4:56–58, 4:66–5:3. "When the signatures are verified, the software application Y 14 can be executed on the device and access any APIs for which corresponding signatures have been verified." *Id.* at 5:9–11.

The '868 patent also describes a method for "network operators" to "maintain control over which software applications are activated on mobile devices." *Id.* at 1:44–46. "In this multiple-signature scenario, all APIs are restricted and locked until a 'global' signature is verified for a software application." *Id.* at 4:1–3. For example, corporate mobile devices may "be configured to require verification of at least a global signature before a software application can be executed," and "[a]ccess to sensitive device APIs and libraries . . . could then be further restricted, dependent upon verification of respective corresponding digital signatures." *Id.* at 4:7–12.

Independent claims 1 and 76 of the ’868 patent, which exemplify the subject matter of the challenged claims, are the only independent claims challenged and are reproduced below:

> 1. A mobile device containing software instructions which when executed on the mobile device cause the mobile device to perform operations for controlling access to an application platform of the mobile device, the operations comprising:
>
> storing a plurality of application programming interfaces (APIs) at the mobile device, wherein at least one API comprises a sensitive API to which access is restricted;
>
> receiving, at the mobile device, an indication that a software application on the mobile device is requesting access to the sensitive API stored at the mobile device;
>
> determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using a private key of a private key-public key pair, wherein the private key is not accessible to the mobile device;
>
> the mobile device using a public key of the private key public key pair to verify the digital signature of the software application; and
>
> based upon verifying the digital signature at the mobile device, the mobile device allowing the software application access to the sensitive API.

Ex. 1001, 14:42–62.

> 76. A method for controlling access to an application platform of a mobile device, comprising:
>
> storing a plurality of application programming interfaces (APIs) at the mobile device, wherein at least one API comprises a sensitive API to which access is restricted;
>
> receiving, at the mobile device, an indication that a software application on the mobile device is requesting access to the sensitive API stored at the mobile device;

> determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using a private key of a private key-public key pair, wherein the private key is not accessible to the mobile device;
>
> mobile device using a public key of the private key-public key pair to verify of [*sic*] the digital signature of the software application; and
>
> based upon verifying the digital signature at the mobile device, the mobile device allowing the software application access to the sensitive API.

Id. at 20:4–22.

II. ANALYSIS

A. Level of Skill in the Art

The level of skill in the art is a factual determination that informs the claim construction analysis and helps guarantee objectivity in an obviousness analysis. *See Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 1323 (Fed. Cir. 1999) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966); *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015) (explaining that claim construction seeks the meaning "a skilled artisan would ascribe" to the term "in the context of the specific patent claim").

Petitioner asserts that a person of ordinary skill in the art at the time of the alleged invention "would have had at least a Bachelor's degree in computer science or the equivalent, and two years of work experience in the relevant field, e.g., secure systems, including security protocols for software applications" and that "[m]ore education can substitute for practical experience and vice versa." Pet. 6. Patent Owner asserts "[o]ne of ordinary skill [] in the field . . . would have had (1) at least a bachelor's degree in computer science, or the equivalent, and (2) at least two years of experience

in secure systems, including security protocols for software applications." PO Resp. 5.

The parties' proposals are similar and neither party argues that it makes a difference which one we choose. We determine that the selection of one proposal over the other does not affect our analysis, but adopt Patent Owner's formulation for purposes of this Decision.

B. Claim Construction

In *inter partes* reviews filed before November 13, 2018, the Board construes claims in an unexpired patent according to their broadest reasonable construction in light of the specification of the patent in which they appear. *See Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016); *Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board*, 83 Fed. Reg. 51,340 (Oct. 11, 2018). The broadest reasonable construction is the "ordinary and customary meaning" to a person of ordinary skill in the art at the time of invention. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc). "[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Phillips*, 415 F.3d at 1313. "[T]he claims themselves provide substantial guidance as to the meaning of particular claim terms," *id.* at 1314, and "[w]hile we read claims in view of the specification, of which they are a part, we do not read limitations from the embodiments in the specification into the claims," *Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F.3d 1367, 1371 (Fed. Cir. 2014). We may "depart from

the plain and ordinary meaning of claim terms based on the specification in only two instances: lexicography and disavowal." *Id.*

1. "signed software application"

All challenged claims include a "signed software application." Patent Owner argues "a POSA would understand a signed software application to be a software application that is signed, i.e., the signature is of the software application or a unique transformation of the software application, such as a hash or an abridging function." PO Resp. 14–15. Specifically, Patent Owner argues [A] "[t]he claims expressly require the software application be digitally signed" (*id.* 7–8), [B] "[e]very example of generating a signed message or a signed software application in the '868 patent involves signing the information to be signed or a unique transformation of that information, such as a hash or abridged version" (*id.* at 8–11), [C] "[t]he extrinsic record and the testimony of Petitioner's expert, Dr. McDaniel, further confirm Patent Owner's construction" (*id.* at 11–13), and [D] "Patent Owner's construction is further confirmed by Petitioner's prior art" (*id.* at 13–14).

Petitioner replies that "while the signed information may need to be associated with the application, the plain and ordinary meaning of the claims does not require signing the application code itself" and "[t]his understanding of the claims is confirmed by the specification of the '868 patent." Reply 2. Petitioner further argues that Patent Owner's arguments based on Dr. McDaniel's testimony are "misplaced," and that the prior art cited by Patent Owner is not contrary to Petitioner's position. *Id.* at 2–3.

We begin the claim construction inquiry "with the actual words of the claim." *Homeland Housewares, LLC v. Whirlpool Corp.*, 865 F.3d 1372,

1375 (Fed. Cir. 2017). Here, claim 1 recites "determining . . . whether the software application is signed" where "a signed software application includes a digital signature generated using a private key of a private key-public key pair, wherein the private key is not accessible to the mobile device." The claim language thus neither requires nor suggests that the signature is "of the software application or a unique transformation of the software application, such as a hash or an abridging function." Instead, to the extent other language in the claim sheds light on the issue, it indicates that "a signed software application" is simply an application that "includes a digital signature generated using a private key." We thus conclude that the actual words of the claim do not support Patent Owner's construction.

We next look to the rest of the intrinsic record, which in this case is the remainder of the specification, and then to "extrinsic evidence [if] appropriate." *Phillips*, 415 F.3d at 1314.

The specification describes the generation of the signed software application as follows:

> If the code signing authority 16 determines that software application Y 14 may access the sensitive API and therefore should be signed, then a signature (not shown) for the software application Y 14 is generated by the code signing authority 16 and appended to the software application Y 14. The signed software application Y 22, comprising the software application Y 14 and the digital signature, is then returned to the application developer 12. The digital signature is preferably a tag that is generated using a private signature key 18 maintained solely by the code signing authority 16. For example, according to one signature scheme, a hash of the software application Y 14 may be generated, using a hashing algorithm such as the Secure Hash Algorithm SHA1, and then used with the private signature key 18 to create the digital signature. In some signature schemes, the private signature key is used to

> encrypt a hash of information to be signed, such as software application Y 14, whereas in other schemes, the private key may be used in other ways to generate a signature from the information to be signed or a transformed version of the information.

Ex. 1001, 4:36–55. We do not agree with Patent Owner that its proposed construction is mandated by this portion of the disclosure. The passage states that "a signature . . . for the software application . . . is generated by the code signing authority," without specifying that the signature must be "of the software application or a unique transformation of the software application," or anything else to that effect. The signature is described as "preferably a tag that is generated using a private signature key . . . maintained solely by the code signing authority," again without any requirement that the tag be generated from the "software application or a unique transformation of the software application." We consider this portion of the specification to describe a broadest embodiment that does not require generation of the signature from the application itself.

The Specification goes on to explain that "*for example, according to one signature scheme*" the application may be hashed and the hash may be used to create the digital signature. Ex. 1001, 4:45–50 (emphasis added). It further states that "[i]n some signature schemes," the private key is used to encrypt a hash of information to be signed, "whereas in other schemes, the private key may be used in other ways to generate a signature from the information to be signed or a transformed version of the information." *Id.* at 4:50–55. We view this description as providing *examples* of how the signed application may be generated, not as evidence that the signature must be generated from the application itself. We determine that these examples, in the absence of a clear disavowal of other embodiments, do not limit the

claims. *See Info-Hold, Inc. v. Applied Media Techs. Corp.*, 783 F.3d 1262, 1267 (Fed. Cir. 2015) ("[T]he scope of the invention is properly limited to the preferred embodiment if the patentee uses words that manifest a clear intention to restrict the scope of the claims to that embodiment."). This is particularly true given that the key may be "used to encrypt a hash of information to be signed, *such as software application Y 14*" (Ex. 1001, 4:51–52, emphasis added), which indicates that the signature may be generated by applying the key to something *other than* the software application or a hash of the software application. Once the signature is generated, it is appended to the application, resulting in "a signed software application."

The written description, we conclude, does not provide a basis for limiting the claims in the manner urged by Patent Owner.

We also are not persuaded by Patent Owner's references to Dr. McDaniel's deposition testimony and declaration (*see* PO Resp. 11–13; Ex. 2002, ¶¶ 51–58), because we do not find statements about digital signatures in general to be sufficient to read limitations into the claims of the '868 patent. Moreover, that testimony is not inconsistent with our result, which allows for the signature to be based on "the thing you're signing." The written description described above is broad enough to include creating a signature using any information (so the signature would be based on "the thing being signed," as described by Dr. McDaniel), and then creating a "signed software application" by appending that signature to the application. For similar reasons, we are unpersuaded by Patent Owner's arguments regarding the prior art (*see* PO Resp. 13–14).

As explained above, the ’868 patent describes “a signed application” as an application to which a signature has been appended, but does not require that the signature have been generated from the application. Even if one of skill in the art would have understood that a digital signature must be based on “the thing you’re signing,” we see nothing in the ’868 patent requiring that the “thing” be the application itself. In other words, and to be clear, we find the disclosure to support claims that encompass creating a signature from something that is not the application itself and then appending that signature to the application.

Patent Owner argues the system could be defeated if the signature was not of the entire application. *See* PO Resp. 13. This seems to be a valid technical point but, even if true, it would be insufficient to mandate Patent Owner’s construction because the claims do not require that the system be perfectly secure. The applicant could have claimed a more secure system by narrowing the claims to the embodiment in which the signature is generated from the application or a hash of the application, but elected to pursue broader claims instead.

Considering the intrinsic and extrinsic evidence as a whole, we find they do not support Patent Owner’s proposed construction of “signed software application,” as requiring that the signature is of the software application or a unique transformation of the software application.

2. “determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using a private key of a private key-public key pair”

All challenged claims include the above phrase, which Petitioner argues should be construed to mean “determining, at the mobile device,

whether the software application includes a digital signature generated using a private key of a private key-public key pair *corresponding to an entity with an interest in protecting access to the sensitive API, such as a mobile device manufacturer or other entity that classified the API as sensitive, or from a code signing authority acting on behalf of the manufacturer*." Pet. 7–8 (emphasis added). Petitioner asks us to find that the claims require the key pair to be generated by the mobile device manufacturer or another entity that classified the API as sensitive. Petitioner notes that in a prior district court case, Patent Owner interpreted this phrase to include a key pair generated by an application developer. *See* Pet. 14 (citing Ex. 1010, 20–21). Petitioner goes on to assert, however, that the "petition demonstrates how the prior art discloses the challenged claims under both Petitioner's and PO's interpretations." *Id.* Patent Owner does not address this issue in this proceeding.

As in the institution decision, because we need not interpret this claim language to reach our decision, we decline to do so. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (explaining that terms are construed to resolve a "controversy, and only to the extent necessary to resolve the controversy").

3. "sensitive API"/"non-sensitive API"

Patent Owner argues "[t]he broadest reasonable interpretation of a 'sensitive API' is an API classified as implicating a security concern" and "[t]he broadest reasonable interpretation of a 'non-sensitive API' is likewise an API that is not classified as implicating a security concern." PO Resp. 16. This is so, according to Patent Owner, because the '868 patent "uses the phrase 'sensitive API' to refer to a specific classification of API related to

the security concerns implicated by that API, in that it may be affected by a virus or malicious code in a device software application." *Id.* at 17.

Petitioner responds that Patent Owner's position is "unsupported by the disclosure of the '868 patent" and that the claims "do not mention security" but, instead, "use these terms merely to distinguish between APIs based on access restrictions." Reply 5–6. Petitioner further argues "PO's construction of 'sensitive API' also fails because neither the specification nor the prosecution history of the '868 patent even mentions the phrase 'security concern,'" Patent Owner and its expert "neglect to explain what this phrase means," and "it is also unclear what it means to 'implicat[e]' a security concern." *Id.* at 6.

We do not agree with Patent Owner that "sensitive APIs" should be limited to APIs classified as implicating a security concern and, instead, we construe this term to mean "an API to which access is restricted." (*See* Inst. Dec. 13.[9]) The claims identify "a plurality of application programming interfaces (APIs)," and then identify a subset of those APIs as "sensitive APIs." The subset is those APIs to which access is restricted by use of the private-public key scheme recited in the claims, as opposed to other APIs to which application access is not restricted by that scheme.

---

[9] Having further considered the issue, we omit from this construction "on an application-by-application basis," which we included in the institution decision. That was done in response to Patent Owner's argument concerning the patent's "multiple-signature scenario" (*see* Prelim. Resp. 8–9), but we now conclude the language is not needed. The patent's description of using one global signature to restrict any API access and a second to allow access to only sensitive APIs does not create any potential inconsistency because the independent claims are not directed to the two signature scheme—they recite only one signature.

Patent Owner does not argue that "sensitive API" is a known term of art (*see* Tr. 74:10) and, as Petitioner observes, the term "security concern" does not appear in the patent or its file history. In an effort to support its construction, Patent Owner points to 3:46–62 of the '868 patent, which begins "[p]referably, any API may be classified as sensitive by a mobile device manufacturer, or possibly by an API author, a wireless network operator, a device owner or operator, or some other entity that may be affected by a virus or malicious code in a device software application." We read this language as indicating that "any API" may be classified as sensitive, not just APIs that "implicate security concerns." We find this to describe an embodiment in which APIs that do *not* "implicate security concerns" may be "sensitive APIs." It is true that the patent states "[f]or instance, a mobile device manufacturer may classify as sensitive those APIs that interface with cryptographic routines, wireless communication functions, or proprietary data models such as address book or calendar entries," but we read that additional language as exemplary ("for instance"), not limiting. Given the lack of any clear indication in the '868 patent of an intent to limit "sensitive APIs" to only APIs that implicate a "security concern," we decline to do so. *See Info-Hold*, 783 F.3d at 1267.

The '868 patent, which does not even use the phrase "security concern," offers no guidance on what the term means, or how one would determine whether or not an API "implicate[s] security concerns." And Patent Owner is also unable to adequately explain it. For example, at the hearing, when asked whether "preventing someone who has not paid a license to access APIs" would be a "security concern," Patent Owner answered in the negative, because "[i]t would be a business concern." Tr.

72:21–73:3. But we fail to see why preventing someone from avoiding the payment of license fees does not "implicate a security concern." The construction we adopt, on the other hand, provides a clear distinction: an API to which application access is restricted using the claimed scheme is a "sensitive API," and an API to which application access is not restricted using that scheme is not a "sensitive API."

As discussed above, the '868 patent is concerned with *both* "ensur[ing] that a software application written by a third party for a mobile device will properly interact with the device's native applications and other resources" *and* the "serious risk that destructive . . . software applications may be downloaded and installed." Ex. 1001, 1:37–43. The specification also describes how the signing authority may determine whether to sign a developer's key based on "several criteria," including "whether or not the developer has a contractual obligation or has entered into some other type of business arrangement with a device manufacturer" (Ex. 1001, 10:11–23), indicating that a valid signature may be provided for API access based on business, as opposed to security, considerations. These disclosures support the conclusion that a "sensitive API" is simply one to which access is restricted—including because a developer has not contracted to access a particular API, because it has not proven that the application properly uses the API, or for any other reason—rather than only because access to the API presents a "security concern."

We are not persuaded by Patent Owner's argument regarding "the role of trust in granting access to sensitive APIs." PO Resp. 18. The '868 patent describes how the signing authority may consult a database or other records to determine whether to "trust" the application developer. But the

determination of whether to trust, and therefore grant access, is made according to several criteria including, as noted above, "whether or not the developer has a contractual obligation or has entered into some other type of business arrangement with a device manufacturer." Ex. 1001, 10:19–22. Again, this suggests that access to the APIs may be allowed for various reasons, including because the developer has contracted for the right to use the APIs, not only because the application having access to the API implicates a "security concern."

As in the institution decision, we find that the claims were drafted using the term "sensitive APIs" as a label, or shorthand, for the subset of APIs to which access is restricted using the scheme described in the independent claims, such that when the claims subsequently refer to the subset they use the shorthand "sensitive API," rather than the entire phrase "sensitive API to which access is restricted."

Patent Owner disputes the notion that the term functions as a label by citing the portion of the patent concerning the additional, global signature, and arguing "the '868 patent describes access restrictions for 'non-sensitive' APIs, despite the Board's implication that 'nonsensitive' would be a label for APIs to which access is not restricted." PO Resp. 19. Patent Owner further argues that the patent describes "different levels of access control . . . a first level that applies to both sensitive and non-sensitive APIs, and a second level that applies to sensitive APIs only." *Id.* at 19. These different levels are, according to Patent Owner, "inconsistent with the interpretation that 'sensitive' is a label for access restricted APIs," and "instead consistent with 'sensitive' as an API classification for APIs that implicate a security concern." *Id.* at 19–20. We do not agree. The fact that the '868 patent

describes the possible use of an *additional* signature to protect *all* APIs is not inconsistent with our interpretation of "sensitive APIs" as those that are individually protected, at a lower level, by the scheme described in the independent claims.

Patent Owner relatedly argues that "equating 'sensitive API' with 'access-restricted API' is also contrary to dependent claim 112, which recites that, 'upon verifying the digital signature at the mobile device, the mobile device allowing the software application access to at least one non-sensitive API.'" PO Resp. 20. We are not persuaded that this supports Patent Owner's desired claim construction. Independent claim 76 recites a system that controls access to individual APIs using a signature and a public key. It uses the digital signature to allow access to certain APIs (the "sensitive" APIs) but not others (those APIs that are not "sensitive"). Claim 112 depends from claim 76 and further recites "upon verifying the digital signature . . . allowing the software application access to at least one non-sensitive API." Claim 112 thus appears directed to a system in which *one* signature allows access to both sensitive APIs (as in parent claim 1) and non-sensitive APIs (as in claim 112). The specification, however, describes an embodiment that uses a *first* signature to control access to sensitive APIs, and a "global" embodiment that would add a *second* signature to initially control access to all APIs. We do not find an embodiment that uses a single signature to allow access to both non-sensitive APIs and sensitive APIs. Because interpreting claim 112 to cover a system in which *one* signature allows access to both sensitive APIs and non-sensitive APIs does not appear

to be supported in the original disclosure,[10] we do not agree that it may appropriately be used to support Patent Owner's narrowing claim construction for claim 1.

Considering the patent disclosure as a whole, as well as the other evidence presented by Patent Owner, we find the record insufficient to require that the "sensitive" designation in the claims be limited to APIs that "implicat[e] a security concern."

4. "[a] plurality of [APIs] . . . , wherein at least one API comprises a sensitive API to which access is restricted"

In the Preliminary Response, Patent Owner asked that we find the claims to require that "'sensitive API[s]' have greater 'access [] restrict[ions]' relative to those 'plurality of APIs' that may be non-sensitive." Prelim. Resp. 9–10. We did not agree in our institution decision that this language requires any additional construction, and Patent Owner does not revisit the issue in the Response. *See* Inst. Dec. 12–13; PO Resp. 5–22. To the extent Patent Owner is still seeking this construction, we decline to add the additional language for the reasons provided in the institution decision. *See* Inst. Dec. 12–13.

---

[10] Claim 112 was added by amendment on November 11, 2011, as application claim 277. *See* November 11, 2011 Amendment (Ex. 1004, 299–326). The accompanying remarks characterized the amendment as "based on features described at, for example, paragraph 34 and Figure 3 of the published application." *Id.* at 23 (Ex. 1004, 321). Paragraph 34 of the application corresponds to column 7, lines 1–32 of the '868 patent, which describe Figure 3. Neither the cited passage nor the figure mentions or otherwise supports using a single signature to control access to both sensitive and non-sensitive APIs.

5. "abridged version of a software application"

Patent Owner argues the broadest reasonable interpretation of "abridged version of a software application," which appears in claim 86, "is a unique transformation of the software application that is smaller than the software application." PO Resp. 21. To support this argument, Patent Owner points to the description in the patent of "an 'abridging scheme or algorithm,' which is used like a hash function to 'generate different outputs for different inputs.'" *Id.* at 21–22 (quoting Ex. 1001, 6:32–37).

Petitioner responds that the patent "does not claim any abridging scheme or algorithm," that "the term 'transformation' is not defined by the specification . . . or by PO and therefore is vague and ambiguous," and that "the specification [does not] refer to an abridged version of the software application as a transformation." Reply 9.

We agree with Patent Owner that the broadest reasonable interpretation of an "abridged version of a software application" is "a unique transformation of the software application that is smaller than the software application." The patent describes an embodiment in which the software developer may "provide the software application Y in some type of abridged format" in order to "have the software application Y signed without revealing proprietary code to the code signing authority." Ex. 1001, 6:16–29. The '868 patent further states "the abridged version may . . . be used to generate the digital signature, *provided that* the abridging scheme or algorithm . . . generates different outputs for different inputs," to "ensure that every software application will have a different abridged version and thus a different signature that can only be verified when appended to the particular corresponding software application from which the abridged

version was generated." *Id.* at 6:34–41 (emphasis added). We conclude that the phrase "provided that" is sufficient to limit claims reciting an abridged version of the application to abridged versions that are unique. *See Hill-Rom Services*, 755 F.3d at 1372 (explaining that disavowal is appropriate where the specification makes clear that the invention does not include a particular feature or is clearly limited to a particular form of the invention); *cf. X2Y Attenuators, LLC v. Int'l Trade Comm'n*, 757 F.3d 1358, 1362 (Fed. Cir. 2014) (finding disavowal where the specification stated the feature was an "essential element"); *Andersen Corp. v. Fiber Composites, LLC*, 474 F.3d 1361, 1367 (Fed. Cir. 2007) (finding disclaimer where the specification indicated that for "successful manufacture" a particular step was "required"); *Chimie v. PPG Indus., Inc.*, 402 F.3d 1371, 1385 (Fed. Cir. 2005) (construing claim to include a feature the applicant told the examiner "must be used").

We do not agree with Petitioner that the term "transformation" is "vague and ambiguous" in this context, as it simply refers to the use of a scheme or algorithm to generate an output from an input—transforming the input into the output—as described in the patent. *See* Ex. 1001, 6:16–41.

6. Claim Construction Conclusion

The table below summarizes our resolution of the claim construction issues we decide in this proceeding.

Term	Resolution
signed software application	does not require that the signature be "of the application"

Term	Resolution
sensitive API / non-sensitive API	"an API to which access is restricted" / "an API to which access is not restricted"
abridged version of a software application	"a unique transformation of the software application that is smaller than the software application"

C. Obviousness

Petitioner contends claims 1, 13, 76–95, 98, 100, 104, 108, 112, 113, 137–139, and 142–144 are unpatentable. *See* Pet. 14–64; Reply 10–21. Patent Owner disputes those contentions. *See* PO Resp. 24–57.

1. Legal Standard

A claim is unpatentable 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. *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 ordinary skill in the art; and (4) objective indicia of nonobviousness. *Graham*, 383 U.S. at 17–18.[11] An assertion of obviousness "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal

[11] As there is no evidence of objective indicia of non-obviousness, our analysis is based upon the first three of the four *Graham* factors.

conclusion of obviousness." *KSR*, 550 U.S. at 418 (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *In re Nuvasive, Inc.*, 842 F.3d 1376, 1383 (Fed. Cir. 2016) (a finding of a motivation to combine "must be supported by a 'reasoned explanation'").

2. Overview of Garst

Garst describes "a method and apparatus for enforcing software licenses for resource libraries such as an application program interface (API), a toolkit, a framework, a runtime library, a dynamic link library (DLL), an applet . . . , or any other reusable resource." Ex. 1012, Abstract.

"[A]n access authorization indicator such as a license text string and a corresponding license key are embedded in a program that has been licensed to use a resource library." Ex. 1012, 3:7–10. "The license text string and the license key are supplied, for example, by a resource library vendor to a program developer who wants to use the resource library with an end user program being developed." *Id.* at 3:10–13. "The license text string includes information about the terms of the license under which the end user program is allowed to use the resource library," and "the license key is an algorithmic derivation, such as, for example, a digital signature, of the license text string that is used to authenticate the license text string." *Id.* at 3:14–20.

"The resource library has a checking [routine] for verifying the resource library vendor's digital signature" and "[t]he resource library is unlocked and made available for use with the requesting program only if the license text string is verified as authentic by the resource library." *Id.* at 3:29–33. "Any modification of the license key or the license agreement text string in the requesting software program is detected by the checking routine, causing the resource library to remain locked." *Id.* at 3:37–40.

3. Overview of Gong

Gong is a book concerning Java security, cited by Petitioner in support of its assertion that "it was known in the art that Java technology was being deployed on mobile devices, including 'PDAs' and 'cell phones.'" Pet. 17 (citing Ex. 1016, 23, 242).

4. Gong as Prior Art

Patent Owner argues that Gong is not a prior art printed publication under 35 U.S.C. § 102(b). It is Petitioner's burden to prove that it is, as Petitioner bears the burden of proving unpatentability by a preponderance of the evidence. *See* 35 U.S.C. § 316(e). Patent Owner urges us to find that Petitioner has not proven Gong is prior art due to insufficient evidence of public accessibility. *See* PO Resp. 43–51.

A reference qualifies as a printed publication under § 102(b) if it was "sufficiently accessible to the public interested in the art." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016). If public accessibility is proven, "there is no requirement to show that particular members of the public actually received the information" disclosed in the reference. *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1568–69 (Fed. Cir. 1988). Public accessibility "is determined on a case-by-case basis, based on the 'facts and circumstances surrounding the reference's disclosure to members of the public.'" *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009) (quoting *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004)).

Gong is a book that bears a 1999 copyright date. *See* Ex. 1016, iv. With the Petition, Petitioner offered evidence that the book was received at the North Carolina State University ("NCSU") library and the Library of

Congress. *See* Ex. 1033–1036. In the institution decision, we recognized that the library evidence did not include a specific date that Gong was indexed or cataloged at either library. Inst. Dec. 19. However, viewing the evidence as a whole, we found it sufficient to establish, for purposes of institution, that Gong was publicly available prior to September 20, 2000. *Id.* In particular, we noted that page v of Exhibit 1016, which is the NCSU copy of Gong, includes a series of date stamps indicating that the book was checked out, and thus publicly available, prior to September of 2000. *Id.*

Following institution, Petitioner served more evidence (including Ex. 1038–1045, the "Additional Evidence") regarding the status of Gong as a printed publication. *See* Tr. 83:1–5. Patent Owner did not address the Additional Evidence in its Response, arguing only that the evidence of public accessibility that had been submitted with the Petition was insufficient. *See* PO Resp. 43–51. In the Reply, Petitioner argued the Additional Evidence provided further proof that Gong was publicly accessible. *See* Reply 21–25. Patent Owner then requested a conference call to discuss its desire for authorization to file a motion to strike the portion of the Reply discussing the Additional Evidence. *See* August 13, 2018 Order (Paper 20), at 2. Following the call, we issued an Order in which we declined to authorize a motion to strike, and instead authorized Patent Owner to file a Sur-Reply, limited to addressing the Additional Evidence. *See id.* at 3. Patent Owner did file a paper titled "Sur-Reply," but did not address the merits of the Additional Evidence; instead, Patent Owner argued only that the Additional Evidence was "improper and should not be considered." Sur-Reply 5.

We weighed Patent Owner's concerns regarding the timing of the Additional Evidence following the conference call, and resolved that issue by providing Patent Owner an additional opportunity to address the Additional Evidence. Patent Owner opted to not do so. The Sur-Reply that was filed amounts to an unauthorized motion to strike and, thus, will not be considered. We do note that Petitioner's arguments in the Reply and Additional Evidence properly responded to arguments that Patent Owner raised in the Response regarding the public accessibility of Gong. *See* 37 C.F.R. § 42.23(b); *Valmont Industries, Inc. v. Lindsay Corp.*, 730 Fed. App'x. 918, 922 (Fed. Cir. 2018) ("Our case law makes clear that a petitioner may submit additional evidence in the reply in response to the patent owner response.").

We conclude that Gong was publicly accessible prior to the effective filing date of the '868 patent, September 21, 2000, and, accordingly, is prior art under 35 U.S.C. § 102(b).

The evidence submitted with the Petition shows that Gong is a book with a 1999 copyright date, that it identifies the first printing as occurring in June of 1999, and that it was published by Addison-Wesley, a well-known publisher. Ex. 1016, p. 1–6. We conclude that those facts, coupled with the evidence that it was received by the NCSU library and actually checked out prior to the critical date,[12] are sufficient to establish public accessibility by a preponderance of the evidence.

---

[12] We are not persuaded by Patent Owner's argument that "there is not a shred of evidence in the record regarding what those date stamps could mean." PO Resp. 48. Gong itself states "[the] book is due on the date[s] indicated below" (Ex. 1016, 4), meaning that stamps are dates upon which

Patent Owner's argument focuses on the lack of evidence submitted with the Petition that the book was indexed at the libraries. However, "[w]hile cataloging and indexing have played a significant role in . . . cases involving library references, . . . neither cataloging nor indexing is a necessary condition for a reference to be publicly accessible. *Lister*, 583 F.3d at 1312 (citing *Klopfenstein*, 380 F.3d at 1348). Instead, "[d]epending on the circumstances surrounding the disclosure, a variety of factors may be useful in determining whether a reference was publicly accessible." *Lister*, 583 F.3d at 1312. In this case, we determine that the facts described above, including, in particular, the stamps indicating the book was *actually borrowed* prior to the critical date, are sufficient to establish public accessibility by a preponderance of the evidence. *Cf. Cornell University v. Hewlett-Packard Co.*, 2008 WL 11274580, at *5 (Rader, J., sitting by designation) (N.D.N.Y. May 14, 2008) (relying in part on signatures verifying public access to a thesis).

The Additional Evidence provides further, and substantial, support for the conclusion that Gong was publicly accessible. In particular, it includes evidence that the book was available for purchase by the public on Amazon.com in 1999 and reviewed by a number of individuals on that site in 1999 (Ex. 1039, at 1, 6–7), that the book was the subject of an on-line chat with the author in September of 1999 (Ex. 1040), and that the book was cited in multiple scholarly articles dated prior to the critical date (Ex. 1041 at 4; Ex. 1042 at 13; Ex. 1043 at 17). The Additional Evidence also includes a declaration of the author of the book, Li Gong, stating, among other things,

---

the book was to be returned to the library. The stamps thus show the book was checked out at least once in 2000.

that the book "was released to the public and available for purchase by the public no later than the JavaOne conference in June of 1999, which [he] attended," that the book "was also available for purchase by the public over the Internet in 1999," and that "[he] began receiving royalty payments for sales of Gong in the second half of 1999." Ex. 1045 ¶¶ 5–6. As noted above, Patent Owner has not contested the substance of any of the Additional Evidence.

Because we find the evidence submitted with the Petition sufficient to show the book was publicly accessible, and, further, that the uncontested Additional Evidence confirms that conclusion, we conclude that Gong is available as prior under 35 U.S.C. § 102(b).

5. Independent Claim 1

We conclude that Petitioner has proven, by a preponderance of the evidence, that the subject matter of claim 1, which we address on an element by element basis below, would have been obvious to a person of ordinary skill in the art in view of Garst and Gong.

a. *"[a] mobile device containing software instructions which when executed on the mobile device cause the mobile device to perform operations for controlling access to an application platform of the mobile device"*

Garst describes "a method and apparatus for enforcing software licenses for resource libraries such as an application program interface (API), a toolkit, a framework, a runtime library, a dynamic link library (DLL)." *See* Ex. 1012, Abstract. It thus teaches software instructions for "controlling access to an application platform." Garst does not describe use of the system on a mobile device. Gong, however, describes the use of Java

security schemes on mobile devices and we agree with Petitioner that it would have been obvious to implement Garst's system on a mobile device, a point Patent Owner does not contest. *See* Pet. 16–19; PO Resp. 22–50.

b. "storing a plurality of application programming interfaces (APIs) at the mobile device, wherein at least one API comprises a sensitive API to which access is restricted"

The software libraries for which Garst describes enforcing licenses are located on the device, which is a mobile device in the combination. *See* Pet. 19–20 (citing, e.g., Ex. 1012, Abstract, 1:37–40, Fig. 2). We agree with Petitioner that such application libraries would include "APIs." *See* Pet. 19 (citing Ex. 1012, Abstract, 1:37–40, 1:63–2:2, 2:18–26, 2:61–67, 7:40–41, 9:10–12, 9:16–17, Figs. 2, 3, 5–7, 9–14). At least one of the application libraries, e.g., one for which a software license is being enforced, is "a sensitive API to which access is restricted" because it is one to which access is limited by the digital signature, as described below.

Patent Owner does not dispute that the combination of Garst and Gong would include APIs stored on the mobile device. We are not persuaded by Patent Owner's argument regarding "a sensitive API" (PO Resp. 38–43) because it is based on Patent Owner's construction of that term and, for the reasons detailed above, we do not agree with that construction. We conclude that the combination of Garst and Gong does teach this limitation under our construction.

c. *"receiving, at the mobile device, an indication that a software application on the mobile device is requesting access to the sensitive API stored at the mobile device"*

Garst teaches receipt of an indication that an application is requesting access to the sensitive API. *See* Pet. 21–22 (citing, e.g., Ex. 1012, 6:47–49 ("[T]he process begins with a requesting program making a request to use the resource library at step 700.")). In the combination, the application is on a mobile device and requesting access to an API on the mobile device. Patent Owner does not argue that the combination would not include receipt, at the mobile device, of an indication that a software application is requesting access to one of the APIs.

d. *"determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using a private key of a private key-public key pair, wherein the private key is not accessible to the mobile device"*

After the request to access the API, Garst's method obtains the program's license text and license key. *See* Ex. 1012, 6:49–50. In at least one embodiment, the key "comprises a digital signature of the resource library vendor." *Id.* at 5:23–25. Garst explains that the key (called "LicenseKeyString") can be a digital signature of the text describing the license restrictions (the "LicenseAgreementString") that is "prepared by providing the LicenseAgreementString and a private key of the API vendor to a digital signature process." *Id.* at 9:38–40. Garst thus teaches that the "digital signature [is] generated using a private key of a private key-public key pair." *See* Ex. 1012, 5:41–43 ("The originator digitally signs the resulting message digest, for example by performing an algorithmic

operation on the message digest using the originator's private key.") We agree with Petitioner that it "was known at the time of the alleged invention, [that] digital signatures necessarily involve[d] a pair of related keys—a 'public key' that can be made public and a 'private key' that must remain private to the key owner and/or a trusted third party." Pet. 23 (citing Ex. 1002 ¶¶ 32–34, 39–47, 142; Ex. 1009, 34–35, 37–38; Ex. 1024, 11–12, 14–16; Ex. 1016, 14–15; Ex. 1014, 12:45–59, 12:66–13:3, 13:23–29).

We are not persuaded by Patent Owner's argument that "Garst discloses signing a license string, not a software application, and thus fails to disclose the claimed 'signed software application' or 'determining . . . whether the software application is signed' elements." PO Resp. 24–25. That argument is based on Patent Owner's claim construction requiring that the digital signature be of the application itself. As explained above, however, we determine that the claims are met by a system that appends a digital signature to an application. The application is "signed" because a signature has been applied.

Nor are we persuaded by Patent Owner's argument that "Garst's license key would not be considered a digital signature of the application program." PO Resp. 28. Under our claim construction, the claims do not require that the digital signature be "of the application program." Garst's digital signature meets the requirements of digital signature of the license. That digital signature is then appended to the application, which, again, is sufficient under our claim construction.

Patent Owner also contests Petitioner's theory that it would have been obvious to sign the developer's software application using the API vendor's

private key. *See* PO Resp. 33–38. Because we do not adopt that theory, we need not address Patent Owner's argument on the issue.

e. "the mobile device using a public key of the private key-public key pair to verify the digital signature of the software application"

Garst uses the public key of the pair to verify the digital signature of the application. *See, e.g.*, Ex. 1012, 3:30–33 ("The resource library is unlocked and made available for use with the requesting program only if the license text string is verified as authentic by the resource library."), Abstract, 3:19–40, 5:47–6:22, 6:41–64, 9:59–62, 10:33–39, 11:23–31, 12:8–25. Patent Owner does not dispute that the Garst-Gong combination would include the mobile device using the public key to verify the digital signature.

f. "based upon verifying the digital signature at the mobile device, the mobile device allowing the software application access to the sensitive API"

Garst allows the application to access the sensitive API based upon verifying the digital signature. *See, e.g.*, Ex. 1012, Abstract ("Resource library functions are made available only to a program having an authentic and unaltered license text string."), Abstract, 2:67–3:6, 3:24–38, 5:62–65, 6:9–22, 6:56–7:22, 9:5–12, 11:5–13. Patent Owner does not argue that, in the combination, the mobile device would not allow the software application access to the API based on verifying the digital signature.

6. Independent Claim 76

Claim 76 is a method claim corresponding to the apparatus of claim 1. Specifically, it recites "[a] method for controlling access to an application platform of a mobile device," where the steps of the method are identical to

the claim 1 limitations discussed in Sections II.C.5.*b–f* above. For the reasons described above, and as Patent Owner does not argue claim 76 separately from claim 1, we conclude Petitioner has shown, by a preponderance of the evidence, that claim 76 would have been obvious over Garst and Gong.

7. Dependent Claims

a. Claim 112

Independent claim 76 recites use of a public key to verify the digital signature of a software application and, based upon verifying the digital signature, allowing the software application to access the sensitive API(s). Claim 112 depends from claim 76 and adds that "upon verifying the digital signature . . . , the mobile device allow[s] the software application access to at least one non-sensitive API." Claim 112 thus contemplates the one digital signature allowing access to *both* sensitive APIs and non-sensitive APIs.

At the hearing, Patent Owner explained that claim 112 "would correspond to the global signature that's described in the specification." Tr. 85. This is the "multiple-signature scenario" described in the '868 patent, in which "all APIs are restricted and locked until a 'global' signature is verified for a software application." Ex. 1001, 4:1–3. The patent explains that, for example, all "corporate mobile devices may . . . be configured to require verification of at least a global signature before a software application can be executed" and "access to sensitive device APIs and libraries, if any, could then be further restricted, dependent upon verification of respective corresponding digital signatures." *Id.* at 4:7–12. This scheme involves at least two digital signatures, one that allows access to all APIs (including non-sensitive APIs), and one that subsequently allows

access to the sensitive APIs. As we described above (*see* Section II.B.3), however, it does not appear that the specification includes an embodiment in which verification of *one* signature allows access to *both* sensitive and non-sensitive APIs.

With that background, we turn to the parties' arguments. Petitioner relies on Garst for the digital signature allowing access to both sensitive APIs and non-sensitive APIs. *See* Pet. 47–49. Patent Owner argues that Garst "fails to disclose allowing access to non-sensitive APIs "upon verifying the digital signature," as required by claim 112. PO Resp. 51–52. Petitioner responds that "[t]he use of 'upon' signifies that access is allowed following the occurrence of verification, not that access is allowed or denied based on whether the digital signature is verified" and that "[p]roperly construed, there is no dispute that Garst and the combination of Garst and Gong disclose the limitations of this claim." Reply 17–18.

Considering claim 112 along with the portion of the written description that concerns use of a signature to control access to non-sensitive APIs, we do not agree with Petitioner that "upon" in the claim is merely temporal. Instead, we conclude that the claim concerns use of a signature to restrict access to non-sensitive APIs, even though the disclosed embodiment would require a second signature not present in the claim. We further conclude that Garst, which only restricts access to the sensitive (i.e., licensed) APIs, not all APIs, does not teach or suggest the subject matter of this claim. Accordingly, Petitioner has not shown by a preponderance of the evidence that claim 112 would have been obvious.

b. Claims 77, 79, 80, and 82

Claims 77 and 80 require "*preventing execution* of the software application" "based upon a determination that the software application requesting access to the sensitive API does not include a signature" (claim 77 (emphasis added)) or "based upon a determination that the digital signature is not successfully verified" (claim 80). Claims 79 and 82 go further, requiring "*purging the software application* from the mobile device" based upon "a determination that the software application requesting access to the sensitive API does not include a signature" (claim 79 (emphasis added)) or "a determination that the digital signature is not successfully verified (claim 82).

For this subject matter, Petitioner relies on Davis, which concerns a system for preventing unauthorized modification of BIOS program code embedded in modifiable non-volatile memory devices such as flash memory. Ex. 1013, Abstract. In Davis, "[a] cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade." *Id.* at 2:61–63. "If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used." *Id.* at 4:12–14. It would have been obvious, according to Petitioner, "to modify the system/processes of the Garst-Gong combination so that unverified application code (e.g., code with an invalid or missing digital signature) is purged and prevented from executing, similar to as described in Davis, to improve device security." Pet. 52–53. Petitioner asserts that "such a modification would have improved device security and data storage utilization." *Id.* at 53.

Patent Owner characterizes "Petitioner's position [as being] that if a software application in Garst were missing even a single license, Davis would suggest removing the software application from the system entirely because of security concerns." PO Resp. 53. Patent Owner argues that "Petitioner fails to justify that result in the context of the references," and does not adequately explain why one would incorporate Davis's teachings into the scheme of Garst. *Id.* Patent Owner observes that "[i]n Davis, if the BIOS firmware fails its validation there is no level of access appropriate for the firmware," whereas "in Garst the application could have a valid license to multiple other API libraries." *Id.* Patent Owner also notes that "Garst discloses preserving the integrity of a licensing scheme, not a security system," and "Garst already prevents the application from accessing the API given an invalid license key." *Id.*

Petitioner responds that "PO's argument misses the mark, because it ignores the combination of references and instead attacks the references individually." Reply 18. Petitioner further argues that "in the context of the Garst-Gong combination, incorporating Davis's teachings relating to deleting code if a digital signature is not successfully verified, which, according to Davis, protects against 'intrusive attacks, such as a virus attack,' makes complete sense" because "[a]s Dr. McDaniel explained, 'deleting unverified application code would have provided an added level of security against such attacks, as it would have reduced the risk that potentially malicious code would have been executed at a later time.'" *Id.* at 19 (citing Ex. 1002 ¶ 214).

We do not agree with Petitioner that Patent Owner is attacking the references individually. Instead, the problem is that Petitioner does not

adequately explain why deleting the entire application would make sense in a system like that of Garst. As Patent Owner observes, Garst describes enforcement of a licensing scheme in which, unlike in the case of the Davis BIOS, the missing signature only means that the application lacks a license to certain APIs, not that the entire application is necessarily useless, a threat, or a waste of storage space. *See* Ex. 2002 ¶¶ 110–113.

Because we find Petitioner has not provided a sufficient motivation to combine, we conclude that Petitioner has not shown that claims 78, 79, 80, and 82 are unpatentable as obvious over Garst, Gong, and Davis.

c. Claim 86

Claim 86 depends from claim 76 and adds, among other things, that the digital signature is "generated by applying the private key to a first abridged version of the software application."

Petitioner argues Garst and Gong do "not explicitly disclose that the application is an abridged version," but that "Sibert's techniques include selecting a portion of an application to hash and sign using a key" and "[i]t would have been obvious to a POSA . . . to modify the system/processes of the Garst-Gong combination to implement such features based on the teachings of Sibert." Pet. 57 (citing Ex. 1015, 7:42–51, 20:64–21:2, 21:44–53, 22:14–41, 22:42–62, Figs. 17, 20A–B; Ex. 1019, 11:1–18, 34:15–35:4, 35:23–38:2). Relying on the claim construction we adopted, Patent Owner responds that "Petitioner has advanced no evidence that [the portions of applications Sibert uses] are unique . . . such that the resulting hashed version of those portions is likewise unique." PO Resp. 55–56. Petitioner replies that "even under PO's construction, claim 86 would have been obvious because Sibert describes signing a unique portion of an application."

Reply 19. Specifically, Petitioner points out that Sibert describes how the portions of the application that are hashed and then signed may be "randomly selected to provide a high degree of unpredictability," may be "disjoint" or "overlap arbitrarily," and/or may cover the same portion of application twice. *Id.* at 20 (citing Ex. 1015, 7:42–51, 20:64–21:2, 21:44–53, 21:64–22:6, 22:19–41, Figs. 17, 20A–C).

Randomly selecting portions of the application may result in a different hash. We cannot say, however, that such a process would necessarily end in unique results and, accordingly, conclude that Petitioner has not shown that the combination of Garst, Gong, and Sibert would have rendered claim 86 obvious. We conclude that the technique described in Sibert falls short of describing "a unique transformation of the software application," and Petitioner does not argue, or offer evidence showing, that it would have been obvious to extend Sibert's methods to ensure that every hash is unique.

d. Remaining Dependent Claims

Petitioner provides a detailed explanation of where the cited references teach the features of claims 13, 81, 83–85, 87–95, 98, 100, 104, 108, 113, 137–139, and 142–144. *See* Pet. 51–64. Petitioner provides sufficient reasoning as to why a skilled artisan would have been motivated to combine Garst and Gong, as well as to add the respective teachings of Chang, Wong-Insley, and Haddock. *See* Pet. 16–19, 54–56, 60–64. Patent Owner does not address Petitioner's challenges to these dependent claims separately from its arguments discussed above regarding claims from which they depend.

After reviewing the arguments and evidence of record, we determine that Petitioner has established by a preponderance of the evidence that dependent claims 13, 81, 84–85, 87, 88, 90–93, 95, 98, 100, 104, 108, 113, 137–139, and 142–144 would have been obvious in view of Garst and Gong; that dependent claim 83 would have been obvious in view of Garst, Gong, and Chang; that dependent claim 89 would have been obvious in view of Garst, Gong, and Wong-Isely; and that dependent claim 94 would have been obvious in view of Garst, Gong, and Haddock.

III. CONCLUSION

Petitioner has demonstrated that claims 1, 13, 76, 78, 81, 83–85, 87–95, 98, 100, 104, 108, 113, 137–139, and 142–144 of the ’868 patent are unpatentable.

Petitioner has not demonstrated that claims 77, 79, 80, 82, 86, and 112 of the ’868 patent are unpatentable.

IV. ORDER

For the reasons given, it is:

ORDERED that claims 1, 13, 76, 78, 81, 83–85, 87–95, 98, 100, 104, 108, 113, 137–139, and 142–144 of U.S. Patent 8,489,868 B2 have been shown to be unpatentable;

ORDERED that claims 77, 79, 80, 82, 86, and 112 of U.S. Patent 8,489,868 B2 have not been shown to be unpatentable; and

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

FOR PETITIONER:

Naveen Modi
Joseph E. Palys
Phillip Citroën
John Holley
PAUL HASTINGS LLP
naveenmodi@paulhastings.com
josephpalys@paulhastings.com
phillipcitroen@paulhastings.com
johnholley@paulhastings.com

FOR PATENT OWNER:

Ching-Lee Fukuda
Samuel A. Dillon
SIDLEY AUSTIN LLP
clfukuda@sidley.com
samuel.dillon@sidley.com