UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC,
Petitioner,

v.

BLACKBERRY LTD.,
Patent Owner.

Case IPR2017-01620
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 13, 85, 86, 88, 98, 104, 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 IPR2017-01620
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, 76–86, 88–95, 98, 100, 104, 112, 113, 137, 139, and 142 of U.S. Patent No. 8,489,868 B2 (Ex. 1001, "the '868 patent"), asserting unpatentability on the following grounds (*see* Pet. 2–3):

References	Basis	Challenged Claim(s)
Lin[1]	§ 102(e)[2]	1, 76, 78, 81, 84, 85, 90–92, 95, 104, 113, 137, and 142
Lin and Garst[3]	§ 103(a)	13, 88, and 98
Lin and Davis[4]	§ 103(a)	77, 79, 80, and 82
Lin and Chang[5]	§ 103(a)	83
Lin and Sibert[6]	§ 103(a)	86
Lin and Wong-Insley[7]	§ 103(a)	89
Lin and Haddock[8]	§ 103(a)	94
Lin and Gong[9]	§ 103(a)	93, 100, 112, 139

[1] U.S. Patent No. 6,766,353 B1, July 20, 2004 (Ex. 1011).

[2] Because the effective filing date of the '868 patent is earlier than March 16, 2013, the pre-AIA versions of Sections 102 and 103 control.

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

[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).

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

We instituted an *inter partes* review on all grounds raised in the Petition. *See* Paper 9 ("Inst. Dec.") at 23.

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 IPR2017-01619, 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, 76–84, 89, 90, 91, 92, 93, 94, 100, 113, 137, 139, and 142 of the '868 patent are unpatentable, but has not shown that claims 13, 85, 86, 88, 98, 104, 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, IPR2017-01619, for *inter partes* review of the ’868 patent based on different prior art. Pet. 1. The 1619 petition includes the claims challenged in this petition, plus 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:

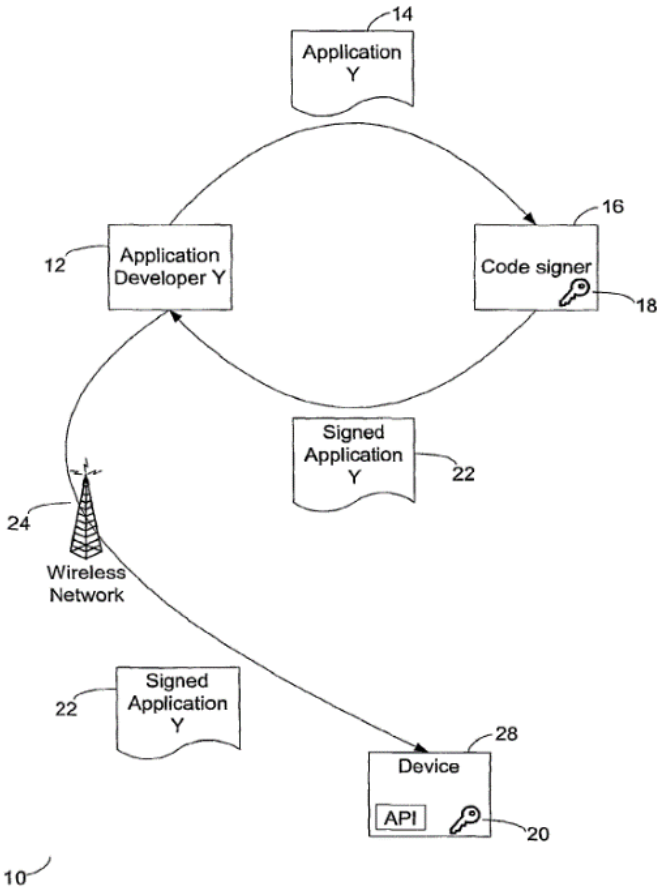

Figure 1

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." *Id.* at 4:56–58. "Once 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 4:66–5:3. "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. "determining, at the mobile device, whether the software application is signed, wherein a signed software application includes a digital signature generated using private key of a private key-public key pair"

All challenged claims include the above phrase. The Petition proposes that this phrase be construed as "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. 8 (emphasis added). Patent Owner did not offer a construction before institution. *See* Prelim Resp. 10–11. At institution, we declined to adopt Petitioner's construction, finding that it unnecessarily narrowed the claims. *See* Inst. Dec. 9–10. Neither the Patent Owner Response nor the Reply substantively addresses this issue.

We find Petitioner's arguments (*see* Pet. 8–12) insufficient to narrow the scope of the claim language because they, at best, seek to limit the claims to the preferred embodiment without identifying anything sufficient to rise to the level of a clear disavowal. *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."). We thus decline to adopt Petitioner's proposed construction and determine that this term does not otherwise require construction.

2. "[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. 7–10. 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.

3. "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. 52. 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.* (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 1–2.

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.

4. Claim Construction Conclusion

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

Term	Construction
abridged version of a software application	"a unique transformation of the software application that is smaller than the software application"

C. Anticipation

Petitioner contends claims 1, 76, 78, 81, 84, 85, 90–92, 95, 104, 113, 137, and 142 are unpatentable as anticipated by Lin. *See* Pet. 15–36; Reply 2–16. Patent Owner disputes those contentions. *See* PO Resp. 10–45.

1. Legal Standard

A claim is anticipated when each and every element is found in a single prior art reference, arranged as recited in the claim. *See Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). "A reference anticipates a claim if it discloses the claimed invention 'such that a skilled artisan could take its teachings in combination with his own knowledge of the particular art and be in possession of the invention.'" *In re Graves*, 69 F.3d 1147, 1152 (Fed. Cir. 1995) (emphasis omitted) (quoting *In re LeGrice*, 301 F.2d 929, 936 (CCPA 1962)).

2. Overview of Lin

Lin concerns a method for authenticating a Java archive for portable devices. Ex. 1011, Title. The method employs "a signed application descriptor file (ADF)" and "a developer descriptor file (DDF)." *Id.* at 2:23–24. The ADF is a file that "describes the portable application in terms of the computing resources it requires" and "is signed by the developer of the corresponding application using a certification authority." *Id.* at 2:23–25, 2:28–32. The DDF is "associated with a particular application software developer" and "specifies the general access control related information assigned to the developer." *Id.* at 2:35–37. "For example, a DDF may restrict the kind of application libraries that applications developed by the developer can use, or the security domain to which the developer belongs." *Id.* at 2:37–40. A signed application descriptor file is shown in Figure 3:

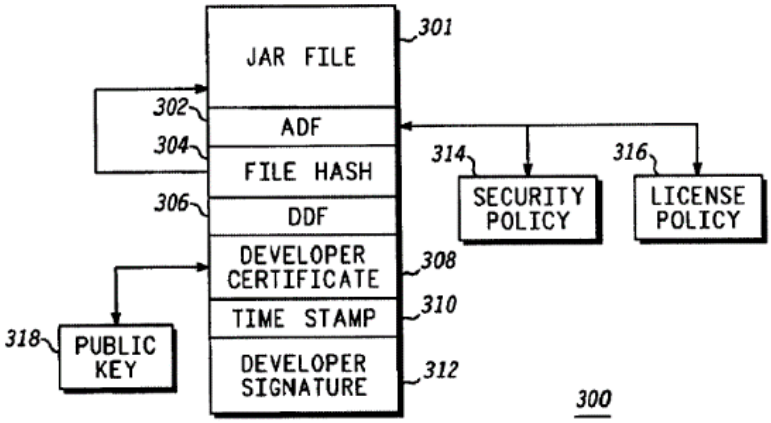

FIG. 3

"FIG. 3 shows a block diagram of a signed application descriptor file (ADF)." Ex. 1011, 1:65–67.

The signed ADF 300 includes a JAR file 301, "containing the portable code to be installed on the client machine," an "application descriptor file 302," a "file hash 304 of the JAR file," a "developer descriptor file

(DDF) 306," a "developer certificate 308," "a time stamp 310," and "a developer signature 312." *Id.* at 3:21–29. "Upon receiving the signed ADF, the client device verifies the developer certificate with the code signing certificate authority's public key (606)." *Id.* at 5:6–8.

3. 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, was anticipated by Lin.

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"

Lin describes "security and authentication of portable code for use by wireless or mobile devices" (Ex. 1011, 1:6–11), where the system may "restrict the kind of application libraries that applications developed by the developer can use" (*id.* at 2:39–40) on the mobile device. *See* Pet. 15–17. Patent Owner does not dispute that Lin satisfies this limitation.

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"

As described above, Lin restricts the kind of application libraries that applications can use on a mobile device. We agree with Petitioner that such application libraries would include "APIs." *See* Pet. 18–20 (citing Ex. 1002 ¶ 142); *see also, e.g.*, Ex. 1011, 2:38–41. 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. *See* Pet. 20–22 (citing, e.g., Ex. 1011, 1:31–35, 2:35–41, 3:5–14, 3:48–56). Patent Owner does not dispute that Lin would include APIs stored on the mobile device or that access is restricted to certain APIs.

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"

Lin teaches receipt of an indication that an application is requesting access to the sensitive API. *See* Pet. 22–23 (citing Ex. 1011, 2:24–29, 3:5–10, 3:12–14, 3:29–31, 3:35–41, 5:26–30, Fig. 3). Patent Owner does not dispute that Lin includes receiving an indication that an application is requesting API access.

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"

Lin determines, at the mobile device, whether the application is signed, using the signed ADF, which includes both the JAR file with the code and the "developer signature 312." *See* Pet. 23–24 ("signed"; citing Ex. 1011, 2:29–32, 3:42–48, 4:15–18, 5:45–48, 6:18–26, 6:58–60; Ex. 1002 ¶ 163); *id.* at 24–26 ("determining"; citing Ex. 1011, 2:29–35, 2:67–3:5, 3:62–64, 4:54–60, 4:66–5:4, 5:6–30, 5:37–52, 6:13–26; Ex. 1002 ¶ 172–175). We conclude that one of skill in the art would have understood the signature to have been generated using the developer's private key, and that the private key would not have been accessible to the mobile device. *See* Ex. 1002 ¶¶ 28–34, 162–169; Section II.C.5.*c*.

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

We agree with Petitioner that Lin describes how "after downloading the application file 204 onto the mobile device, the device verifies digital signature 312 using public key 318." Pet. 28 (citing Ex. 1011, Abstract, 2:29–35, 3:62–64, 5:20–30, 5:43–48, 6:18–20, 5:6–8; Ex. 1002 ¶¶ 177–178). Patent Owner does not dispute that Lin uses 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"*

Lin allows the application to access the sensitive API based upon verifying the digital signature. *See* Pet. 28–29 (citing Ex. 1011, Abstract, 1:6–11, 1:29–39, 1:56–58, 2:20–29, 2:29–41, 3:5–14, 3:12–16 ("The virtual machine only allows the application to access the resources permitted, as dictated by the signed ADF."), 3:21–39, 3:35–39, 3:48–56, 3:63–64, 4:20–23, 5:6–13, 5:20–30, 5:37–52, 5:62–6:61, 6:18–20, Figs. 2, 3). We discuss Patent Owner's argument regarding this "based on" recitation below. *See* Section II.C.5.*b*.

4. 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.3.*b–f* above. Patent Owner does not argue claim 76 separately from claim 1.

5. Patent Owner Arguments Regarding Anticipation

Patent Owner makes three arguments regarding anticipation by Lin, which we address in the order presented.

a. Improperly Combining Embodiments

Patent Owner first argues that Petitioner improperly combines distinct embodiments described in Lin. *See* PO Resp. 17–25. We disagree because, viewed as a whole, Lin describes one system that can be implemented in various ways. Lin's description begins with a general overview (*see* Ex. 1011, 2:19–41), describes in connection with Figure 1 the types of hardware and software that may used (*see id.* at 2:42–64), describes in connection with Figure 2 the network environment (*see id.* at 2:25–3:20), describes in connection with Figure 3 the ADF (*see id.* at 3:21–64), describes in connection with Figure 4 how the developer produces the ADF (*see id.* at 3:64–4:29), describes in connection with Figure 5 how the developer obtains a developer's certificate (*see id.* at 4:30–53), and then describes in connection with Figure 6 how clients can download the ADF and the application (*see id.* at 4:54–5:30). Although it is true that the portion of the description associated with Figure 6 does not specifically state that the ADF and application may be transferred together, we find that immaterial because the overall system is described as including the option for them to be transferred together. *See* Ex. 1011, 3:1–5 ("[T]he client device [receives] an application file 204, which includes a signed ADF 206 and the application code 208. . . . *These two parts maybe transferred separately or together*." (emphasis added)). Because Figure 6 and its associated description purport to detail only a portion of the overall system, not a standalone embodiment, there is no improper mixing of embodiments.

b. "Based Upon Verifying the Digital Signature"

Patent Owner next argues that the claim language "based upon verifying the digital signature at the mobile device, the mobile device allowing the software application access to the sensitive API" means that "access to the sensitive API [depends] on successful verification of the digital signature" and that Lin "does not disclose that an application's access to device resources 212 is 'based upon verifying' digital signature 312." PO Resp. 25–26. Patent Owner argues that "even if the process for verifying digital signature 312 were inherently disclosed, such disclosure does not in turn disclose—either expressly or inherently—that a software application is allowed to access resources 'based upon verifying' digital signature 312." *Id.* at 27. Regarding Lin's disclosures that the "developer's signature . . . allows the client device to authenticate the ADF" (Ex. 1011, 3:63–64) and that the "developers provide[] their public key in the signed ADF so that client devices can use them to further establish a trusted chain" (*id.* at 5:43–45), Patent Owner argues that these passages "say nothing about whether execution of the . . . application is 'based upon' successful verification of developer's digital signature 312." PO Resp. 27.

Petitioner responds that "as explained by Dr. McDaniel, verification of signature 312 using the developer's public key 318 confirms that elements 302/304/306/308/310 have not been altered after signature 312 was created" and that "the 'signed ADF allows devices . . . to easily authenticate the trustworthiness of an application' before it is executed." Reply 8–9 (quoting Ex. 1011, 5:37–40).

We agree with Petitioner that Lin describes allowing the software application access to the sensitive API "based upon" verifying the digital

signature 312. Having considered Lin's description as a whole, as well as the expert testimony on this issue (*see* Ex. 1002 ¶¶ 179–182; Ex. 2002 ¶¶ 62–75), we conclude that one of skill in the art would have understood that the purpose of verifying the digital signature 312 would have been to make a determination about whether the ADF was trustworthy or had been altered. We further conclude that one of skill in the art would have known not to rely on the ADF to allow access by the application if the digital signature could not be verified. We see no other purpose for the digital signature 312, and, when asked at the hearing, Patent Owner likewise could not identify one. *See* Tr. 93:22–94:6. In fact, Patent Owner acknowledged that the digital signature 312 "could potentially provide an additional level of assurance" (*id.* at 94:1–2), and we understand that to mean, in this context, that insufficient assurance would cause one to not allow access by the application.

Our conclusion is also supported by Lin's claim 2, which adds to the "method of authenticating a JAVA archive file as defined in claim 1," the additional step of "verifying the developer signature using the developer public key." Patent Owner's argument that claim 2 shows "that Lin's system does not require verification of the developer signature at all" (*see* Ex. 2002 ¶ 75) is not persuasive because the salient question is whether the concept is disclosed, not whether it is required in every embodiment.

We, accordingly, conclude that Lin *does* disclose that an application's access is "based upon verifying" digital signature 312.

c. Private Key Not Accessible to the Mobile Device

Patent Owner's third argument is that it is not inherent in Lin that the mobile device does not have access to the developer's private key. To

support this contention, Patent Owner suggests that "the client device that downloads the signed ADF and application could belong to the same developer who signed the ADF and, in that scenario, the mobile device would be trusted." PO Resp. 33.

Petitioner responds that "Lin describes a conventional digital signature scheme where the client device must verify signature 312" and that "a POSA would have understood that the private key is not accessible to the client device." Reply 12. Petitioner argues that if the key was accessible, "Lin's security measures would be compromised and the digital signature could not be verified with confidence." *Id.* at 11–12.

We do not agree that one must resort to inherency to find anticipation on this record. Lin describes the use of a public key to verify the developer's signature, a description that one of skill in art would recognize to require a private key that is private to the developer. (*See* Ex. 1002 (McDaniel Decl.) ¶ 33 ("These algorithms are called 'public-key' because the public key can be made public, while the private key remains secret."); Ex. 1046 (Ligler Tr.), 66:18–21 ("The general idea of a public/private key pair is that one would use one's private key, which was known in the abstract only to one's self, access to it was very limited."); Tr. 112–13 (Q: "What's the point of a private key?" PO Counsel: "So the point of a private key is for it to remain private. . . .").

Moreover, even if we did need to resort to inherency, we would still find the reference sufficient to anticipate because, in order for Lin's authentication system to work properly, the developer's key must be private to the developer and, thus, "not accessible to the mobile device." It cannot

reasonably be disputed that a secure system requires, in practice, that the private key be private. *See* Ex. 1002 ¶¶ 28–34, 162–169.

We do not agree that the application developer having the key and putting the application on the developer's device with access to the key for "testing" is a realistic scenario, because we fail to see how one could usefully test the authentication system if the key were accessible. Further, as we noted in the institution decision, "it is unclear why . . . the private key would be on a developer's mobile device, as opposed to being on a personal computer or other, non-mobile hardware more likely to be used for development and/or the application of digital signatures." Inst. Dec. 17. Patent Owner argues that the claim only requires the key to be "accessible," and it would "be 'accessible' to the developer's mobile device because the developer has access to his/her own private key." PO Resp. 34–35. We do not, however, see why the *developer* having access to the key necessarily means that it would be accessible to the developer's *mobile device*, particularly given that, as noted, testing the system as it would work in practice would require that the mobile device *not* have access to the key. *See* Ex. 1002 ¶¶ 28–34, 162–169.

We conclude that the scenario posited by Patent Owner—which is not described in the patent, which is not plausible, and which would not be one in which Lin's system would work for its intended purpose—is not sufficient to defeat inherency. *See MEHL/Biophile Int'l Corp. v. Milgraum*, 192 F.3d 1362, 1365 (Fed. Cir. 1999) (explaining that inherency is based on "the natural result flowing from the operation as taught [in the reference]") (quoting *In re Oelrich*, 666 F.2d 578, 581 (CCPA 1981)).

6. Dependent Claims 78 and 81

Claims 78 and 81 depend from claim 76 and add "denying the software application access to the sensitive API" based on "a determination that the software application requesting access to the sensitive API does not include a signature" (claim 78) or "based upon a determination that the digital signature is not successfully verified" (claim 81).

Petitioner argues "Lin discloses these features" as, "for example, upon receiving signed ADF 206, Lin's mobile device 'authenticate[s] the signed time stamp' (step 608) . . . which is used by the mobile device 'to check whether the ADF file is signed within the valid period of the developer certificate." Pet. 29 (citing Ex. 1011, 3:56–61, 4:7–12, 5:6–12, Fig. 6; Ex. 1002 ¶¶ 183–186). Petitioner asserts that "[t]he signed timestamp 'must be verified' (i.e., the ADF must include signature 312 generated within the valid period), or else the application cannot be executed according to developer permissions, and therefore may be denied access to some or all of resources 212." *Id.* at 29–32 (citing Ex. 1011, 5:12–13). Petitioner further argues "Lin also describes verifying signature 312" and "[i]f the ADF file is signed within the valid period and signature 312 is verified, the application may be loaded into VM 214 for execution according to developer permissions," but "[o]therwise, the application is not executed according to developer permissions, and therefore may be denied access to some or all of resources 212." Pet. 30 (citing Ex. 1011, Abstract, 1:24–38, 2:29–41, 3:5–14, 3:63–64, 4:20–23, 5:12–13, 5:20–30, 5:37–40, 5:43–48, 6:18–20; Ex. 1002 ¶ 184). Petitioner further argues "it would be impossible to verify signature 312 if the application does not include the signature," because "signature 312 must be successfully verified in order for an application to be

executed according to developer permissions" and "an application would also be denied access to some or all of resources 212 if the application does not include signature 312." Pet. 30 (citing Ex. 1002 ¶ 185).

Patent Owner argues "[w]ith respect to claim 78, Lin does not disclose 'a determination that the software application requesting access to the sensitive API does not include a signature' because Lin does not disclose any embodiments where the signed ADF that the client device receives—whether with or separate from the software application—'does not include a signature.'" PO Resp. 37 (citing Ex. 2002 ¶ 84; Ex. 2004, 215:3–6). According to Patent Owner, "[b]ecause Lin does not disclose any embodiments where the signed ADF does not include a signature, Lin also cannot disclose any 'determination' that the signed ADF 'does not include a signature,' let alone how Lin's system would behave if the signed ADF did not include a signature." *Id.* (citing Ex. 2002 ¶ 84).

With respect to claims 78 and 81, Patent Owner argues that "[w]hile Lin discloses how Lin's system behaves if various elements of the signed ADF are successfully verified (e.g., developer certificate, signed timestamp), there is no disclosure in Lin of how Lin's system behaves if those elements are not successfully verified" and "there is certainly no disclosure of how Lin's system behaves if developer signature 312, on which Petitioner relies, were not successfully verified." PO Resp. 38 (citing Ex. 2002 ¶¶ 85–87). According to Patent Owner, "[t]hat Lin discloses the conditions that must be satisfied before a software application is permitted to execute and access resources 212 does not mean that Lin necessarily discloses what happens if those conditions are not satisfied," as "[f]or example, even if the elements of the signed ADF are not successfully verified, Lin's system could provide the

user of the client device with final control over whether to nevertheless permit the software application to access resources 212." *Id.* (citing Ex. 2002 ¶¶ 89–90).

Patent Owner further argues that "[w]hile Lin does disclose that the signed time stamp 'must be verified' . . . , Lin does not similarly disclose that the developer's digital signature 312, on which Petitioner relies as the claimed digital signature . . . , must also be verified in order for the client device to allow the application to access resources 212." PO Resp. 39.

Petitioner responds that "verification of time stamp 310 determines whether the application includes a signature 312 generated within the valid period, which discloses the limitations of claim 78," and also that "[v]erification of signature 312 is required before the application is loaded for execution . . . and it would be impossible to verify signature 312 if it is not included." Reply 13–14.

We agree with Petitioner that Lin anticipates claims 78 and 81. As explained above, Lin describes allowing the application access if the signature can be verified. We conclude that one skilled in the art would have understood that to mean *not* granting access if the signature could *not* be verified, and also would have understood that a signature that was not present could not be verified. *See* Ex. 1002 ¶¶ 183–185.

7. Dependent Claims 85 and 104

In claim 85, which depends from independent claim 76, the digital signature is "generated by applying the private key to a first hash of the software application," and then verified "by generating a second hash of the software application to obtain a generated hash, applying the public key to the digital signature to obtain a recovered hash, and verifying that the

generated hash and the recovered hash are the same." In claim 104, which also depends from claim 76, verifying the digital signature includes "hashing the software application to obtain a generated hash; applying the public key to the digital signature to obtain a recovered hash; and comparing the generated hash and the recovered hash."

Petitioner argues that Lin discloses these features in that "developer signature 312 ('digital signature') is created by signing a hash of elements 302/304/306/308/310 ('first hash of the software application') using the developer's private key ('the private key)" and "a POSA would have understood" that the digital signature "is necessarily verified by applying public key 318 ('public key') to signature 312 to obtain the hash of elements 302/304/306/308/310 ('recovered hash'), generating a hash of the same elements ('second hash'/'generated hash'), and verifying that the two hash files are the same." Pet. 32–33 (citing Ex. 1011, Abstract, 2:29–35, 3:62–64, 5:26–30, 5:43–48, 6:18–20; Ex. 1002 ¶ 190); *see* Pet. 35 (relying on the analysis of claim 85 to establish the obviousness of claim 104).

Patent Owner argues that "developer signature 312 is generated by applying a private key to a hash of a collection of elements, including ADF 302, file hash 304, DDF 306, developer certificate 308, and time stamp 310, not by applying a private key to a 'hash of the software application,' as required by claim 85." PO Resp. 41. Patent Owner further argues that "because digital signature 312 was generated by applying a private key to a hash of [the concatenated elements], the only way to verify digital signature 312 is by recovering the hash of [the concatenated elements] using the developer's public key, generating a hash of [the concatenated elements], and comparing the recovered and generated hashes," "but claims 85 and 104

require the generated hash to be a hash *of the software application*." *Id.* at 42. In other words, "[a] hash of elements 302, 304, 306, 308, and 310 is not a 'hash of the software application,' as required by the claims," and [a] hash of file hash 304 itself would be "a hash of a hash of the software application, not a hash of the software application." *Id.* at 42–43.

Petitioner responds that "the challenged claims do not preclude the 'hash of the software application' from including additional information" and "[a]dditionally, a hash of a hash of the software application is still a hash of the software application, as a hash is simply a fixed-length, cryptographic representation of data." Reply 15.

We agree with Patent Owner. The plain language of these claims requires hashing the application. Petitioner acknowledges that Lin does not hash the application itself, and we agree with Patent Owner that a hash of a hash of an application is not the same as a hash of the application. A hash "take[s] a variable-length input and convert[s] it to a fixed-length output, which is typically much smaller than the input" (Ex. 1002 ¶ 43), meaning that a hash of an application will have a certain length, and a hash of that hash will be necessarily be a smaller, and therefore different, thing. Lin, therefore, does not anticipate claims 85 and 104. *See Net MoneyIN*, 545 F.3d at 1371 (requiring "all of the limitations arranged or combined in the same way as recited in the claim" for anticipation).

8. Dependent Claim 95

Claim 95 adds to claim 76 that "the digital signature provides an audit trail identifying a developer of the software application requesting access to the sensitive API."

Petitioner argues "Lin discloses that the developer's signature 312 includes a DDF 306 ('audit trail') and developer's certificate 308 ('audit trail'), each of which identifies the developer of the application requesting access to the sensitive API." Pet. 35 (citing Ex. 1011, 2:35–38, 3:48–56, 4:12–20; Ex. 1002 ¶ 197).

Patent Owner responds that "developer's signature 312 does not 'include[]' the DDF 306 and developer's certificate 308, as Petitioner alleges" because "the DDF 306, developer's certificate 308, and developer's signature 312 are all separate components of the signed ADF." PO Resp. 44. Patent Owner further argues that "although the DDF 306 and developer certificate 308 may identify the developer of the application, claim 95 requires that 'the digital signature' provide an audit trail to the developer, and Petitioner has not established that developer signature 312 provides the claimed audit trail to the developer." *Id.* at 45 (citing Ex. 2002 ¶ 104).

Petitioner responds that "Lin's signature 312 provides the claimed 'audit trail' because it is generated using a hash of elements that identify the developer, including DDF 306 and certificate 308." Reply 15.

We agree with Petitioner that "signature 312 is similar to the digital signatures . . . described in the '868 patent, and that both "provide" an audit trail "identifying" the developer, as claimed. *See* Ex. 1002 ¶¶ 177–178; *compare, e.g.*, Ex. 1011 (Lin), 3:63–64 ("The developer's signature [] allows the client device to authenticate the ADF."), *with* Ex. 1001 ('868 Patent), 10:51–53 ("the digital signature provides an audit trail through which the developer of a problematic software application may be identified"). We, therefore, agree that Lin describes the subject matter of claim 95 and anticipates the claim.

9. Claims 84, 90–92, 113, 137, and 142

Petitioner provides a detailed explanation of where the cited references teach the features of claims 84, 90–92, 113, 137, and 142. *See* Pet. 31, 33–34, 35–36. Patent Owner does not address Petitioner's challenges to these dependent claims separately from its arguments discussed above regarding the 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 Lin anticipates these claims.

D. Obviousness

Petitioner contends the following combinations render the remaining challenged claims unpatentable as obvious under 35 U.S.C. § 103(a): Lin and Garst (claims 13, 88, and 98); Lin and Davis (claims 77, 79, 80, and 82); Lin and Chang (claim 83); Lin and Sibert (claim 86); Lin and Wong-Insley (claim 89); Lin and Haddock (claim 94); and Lin and Gong (claims 93, 100, 112, and 139).

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.[10] 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 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. Dependent Claims 13 and 88

Claim 13 adds to claim 1 that "the operations further comprise . . . displaying a description string when the software application attempts to access the sensitive API." Claim 88 similarly adds to claim 76 "displaying a description string when the software application attempts to access the sensitive API."

Petitioner argues "Lin does not disclose displaying a description string when the software application attempts to access the sensitive API" but "Garst explains that when an unlicensed software application attempts to access a sensitive API, the software application is denied access and an error message is displayed." Pet. 37. According to Petitioner, "it would have been obvious to a POSA to modify Lin's system/processes to execute software instructions to perform operations that implement such features based on the teachings of Garst and the knowledge of a POSA." *Id.*

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

Patent Owner argues that "the point at which Lin's application attempts to access a sensitive API is after Lin's system has already determined that access should be granted" and that "there would be no reason at that point in the process to 'inform the user that an attempted access to an API was denied and why,' as described in Garst." PO Resp. 46–47 (emphasis omitted).

Petitioner responds that "[t]he claims . . . do not state that the string is displayed upon determining that access should be granted but rather when the application actually "attempts to access the sensitive API." Reply 16.

We conclude that Petitioner has not shown how the modification of Lin to incorporate the notifications of Garst would result in the subject matter of claims 13 and 88. Petitioner argues that Garst displays an error message when an unlicensed software application attempts to access a sensitive API and access is denied. *See* Pet. 37 (citing Ex. 1012, 9:59–64, 10:3–6, 10:33–53, 10:62–11:38, 12:3–42, 16:24–44). In Lin's system, however, the authentication check is made upon receipt of the ADF, not when the application attempts to access the API. *See* Ex. 1011, 5:6–8 ("Upon receiving the signed ADF, the client device verifies the developer certificate with the code signing certificate authority's public key (606)."). Therefore, we find that even if it would have been obvious to add a notification like that of Garst to Lin's method, that notification would be made at the time of Lin's failed authentication, before the application is loaded, because authentication failure in Lin means that the application does not load and, thus, would not "attempt[] to access the sensitive API."

We, therefore, conclude Petitioner has not shown by a preponderance of the evidence that it would have been obvious to modify Lin and Garst to achieve the subject matter of claims 13 and 88.

3. Dependent Claim 98

Claim 98 limits claim 76 by adding that "the digital signature is first verified each time the software application requesting access to the sensitive API is allowed to interact with the application platform."

Petitioner argues that "[w]hile Lin does not explicitly describe verifying digital signatures each time the application requests access to a sensitive API in order to interact with the application platform, it would have been obvious to a POSA to modify the device/processes of Lin to incorporate such features based on the teachings of Garst and the knowledge of a POSA." Pet. 39–40. Petitioner asserts that "verifying signature 312 upon each access request" would "improve device security" by "ensur[ing] that the authenticity and integrity of the code remained intact throughout the use of the application, rather than only upon download." *Id.* at 40. According to Petitioner, this modification would have been "nothing more than a combination of known prior art elements . . . using known programming methods without changing their respective functions to achieve a predictable result." *Id.*

Patent Owner contests the motivation, arguing that "verifying digital signature 312, at best, only verifies that the signed ADF has not changed since download" and "does not 'ensure[] that the authenticity and integrity *of the code* remained intact throughout the use of the application,' as Petitioner alleges." PO Resp. 47. Patent Owner also argues "the entire purpose of Lin's system is to account for the 'limited computing resources' on mobile

devices" and "verifying the signature 312 each time the application is loaded would unnecessarily consume the client device's already limited computing resources while providing little added benefit." *Id.* (quoting Ex. 1011, 2:20–24; citing Ex. 2002 ¶ 114) (emphasis omitted).

Petitioner replies that "PO's argument is based on a misunderstanding of Petitioner's obviousness combination and how conventional digital signatures worked." Reply 16. According to Petitioner, "[b]y verifying signature 312, file hash 304 can confidently be compared to a hash of the application code produced by the client device to confirm the integrity of the code, as described in Lin." *Id.* at 17 (citing Ex. 1002, ¶¶ 173–175; Ex. 1011, 5:20–26). With respect to the "limited computing resources" argument, Petitioner explains that "Lin is not concerned about computing resources generally, but rather the amount of storage space on mobile devices" and that "[t]he proposed modification of Lin based on Garst does not involve changing the size of any files." *Id.* (citing Ex. 1011, 1:54–58, 3:14–20, 3:31–35, 5:31–37).

We agree with Patent Owner because we do not see why "verifying signature 312 upon each access request" would ensure that "the authenticity and integrity *of the code* remained intact throughout the use of the application." Pet. 40. In Lin, the client device loads the application into the virtual machine environment for execution "[i]f the hash of the application received in the signed ADF matches the hash of the received application file." Ex. 1011, 5:26–30. In order to test that *the application* has not changed, one would need to hash the application, and compare that hash with the hash that was received in the ADF. *See* Ex. 1001, 5:20–30. The problem with Petitioner's position is that signature 312 verifies only the

ADF, so verifying that signature would show tampering only with the ADF, not tampering with *the application*. *See* Ex. 2002 ¶¶ 113.

We, therefore, conclude Petitioner has not shown by a preponderance of the evidence that it would have been obvious to modify Lin and Garst to arrive at the subject matter of claim 98.

4. Dependent 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) 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) 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. *See* Pet. 41–44; 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.* 2:61–63. "If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used." *Id.* 4:12–14. It would have been obvious, according to Petitioner, "to modify the system/processes of Lin such 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. 42.

Patent Owner argues that "[d]ownloading the signed ADF first and then separately downloading the software application if the signed ADF is verified already provides the advantages Petitioner claims would be gained by modifying Lin in view of Davis." PO Resp. 50.

Petitioner responds that "PO's argument ignores the scenario described in Lin where the signed ADF and application code are transferred together." Reply 18.

We agree with Petitioner. Patent Owner's argument is directed only to the embodiment in Lin in which the ADF is downloaded before the application. Patent Owner does not address the embodiment in which the ADF and application are downloaded together before the ADF is verified. Accordingly, we agree that, on this record, and by a preponderance of the evidence, it would have been obvious to combine Davis with Lin to prevent execution of, or purge, an application that does not have a signature that can be verified, as recited in claims 77, 79, 80, and 82.

5. Dependent Claim 86

Among other things, claim 86 adds to claim 1 that the digital signature is "generated by applying the private key to a first abridged version of the software application."

Petitioner argues "Lin does not explicitly disclose that the software 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 Lin to implement such features based on the teachings of Sibert." Pet. 47

(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; Ex. 1002 ¶¶ 108–111, 229–232). 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. 53. 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 18. 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 18–19 (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 Lin 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.

We, therefore, conclude Petitioner has not shown by a preponderance of the evidence that it would have been obvious to modify Lin and Sibert to achieve the subject matter of claim 86.

6. Dependent Claims 93, 100, 112, and 139

Petitioner alleges that claims 93, 100, 112, and 139 would have been obvious in view of Lin and Gong. Pet. 54–63. Patent Owner argues that Gong is not prior art, and that claim would not have been 112 obvious. *See* PO Resp. 56–64.

a. Gong as Prior Art

We must determine whether Gong is 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. 56–63.

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, 1–6. We conclude that those facts, when coupled with the evidence that it was received by the NCSU library and actually checked out prior to the critical date,[11] are sufficient to establish public accessibility by a preponderance of the evidence.

---

[11] 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. 61. Gong itself states "[the] book is due on the date[s] indicated below" (Ex. 1016, p. 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, 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, 4; Ex. 1042, 13; Ex. 1043, 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).

b. Obviousness

Petitioner provides a detailed explanation of where the cited references teach the features of claims 93, 100, and 139, and adequately explains why a skilled artisan would have been motivated to combine Lin and Gong. *See* Pet. 54–63. Patent Owner does not address Petitioner's challenges to these dependent claims separately from its arguments discussed above regarding the parent claims, and we conclude that Petitioner has established, by a preponderance of the evidence, that these dependent claims also would have been obvious.

Patent Owner does offer a separate argument for claim 112, which 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. It does not appear, however, that the '868 patent specification includes an embodiment in which verification of *one* signature allows access to *both* sensitive and non-sensitive APIs.[12]

With that background, we turn to the parties' arguments. Petitioner relies on Lin for the digital signature allowing access to both sensitive APIs and non–sensitive APIs. *See* Pet. 59–60. Patent Owner argues "the plain language" of claim 112 "expressly requires allowing such access 'upon

---

[12] 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.

verifying the digital signature at the mobile device."" PO Resp. 63. Patent Owner further argues "the combination that Petitioner proposes would . . . fail to meet the claim because access to those 'non-sensitive' resources is not allowed 'upon verifying the digital signature.'" *Id.* Petitioner responds that "[t]he mere 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." Reply 20.

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 the combination argued by Patent Owner would only restrict access to the sensitive (i.e., licensed) APIs, not all APIs, does not teach or suggest the subject matter of this claim, and, accordingly, that Petitioner has not shown by a preponderance of the evidence that claim 112 is obvious.

7. Remaining Claims 83, 89, and 94

Petitioner provides a detailed explanation of where the cited references teach the features of claims 83, 89, and 94, and adequately reasons why a skilled artisan would have been motivated to combine Davis, Chang, Wong-Insley, and Haddock. *See* Pet. 44–47, 50–54. 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 claim 83 would have been obvious in view of Lin and Chang, that claim 89 would have been obvious in view of Lin and Wong-Insley, and that claim 94 would have been obvious in view of Lin and Haddock.

III. CONCLUSION

Petitioner has demonstrated that claims 1, 76–84, 89, 90, 91, 92, 93, 94, 100, 113, 137, 139, and 142 of the '868 patent are unpatentable. Petitioner has not demonstrated that claims 13, 85, 86, 88, 98, 104, and 112 of the '868 patent are unpatentable.

IV. ORDER

For the reasons given, it is:

ORDERED that claims 1, 76–84, 89, 90, 91, 92, 93, 94, 100, 113, 137, 139, and 142 of U.S. Patent 8,489,868 B2 have been shown to be unpatentable;

ORDERED that claims 13, 85, 86, 88, 98, 104, 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