

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CITRIX SYSTEMS, INC.,
Petitioner,

v.

WORKSPOT, INC.,
Patent Owner.

IPR2018-00917
Patent 9,426,182 B1

Before WILLIAM M. FINK, *Vice Chief Administrative Patent Judge*,
THU A. DANG, and CHRISTA P. ZADO, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

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

In response to a Petition (Paper 2, “Pet.”) filed by Citrix Systems, Inc. (“Petitioner”), we instituted *inter partes* review of claims 1–18 of U.S. Patent No. 9,426,182 B1, issued on August 23, 2016 (Ex. 1001, “the ’182 patent”). During the trial, Workspot, Inc. (“Patent Owner”) filed a Response (Paper 14, “PO Resp.”), to which Petitioner filed a Reply (Papers 16, 18, “Reply”). In turn, Patent Owner filed a Sur-Reply. Paper 20 (“Sur-Reply”). An oral hearing was held with the parties on August 19, 2019. A transcript of the hearing has been entered into the record (Paper 29, “Tr.”).

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has not shown, by a preponderance of the evidence, that claims 1–18 of the ’182 patent are unpatentable.

I. BACKGROUND

A. *The ’182 Patent (Ex. 1001)*

The ’182 patent relates to context-based authentication of mobile devices. Ex. 1001, code (54). An access control system receives context of a request, selects an access control policy based on the context of the request, and sends access control information from the access control policy selected to the client, wherein the client then interacts with the user to perform authentication using the access control information. *Id.* at code (57).

Figure 1A of the ’182 patent is reproduced below:

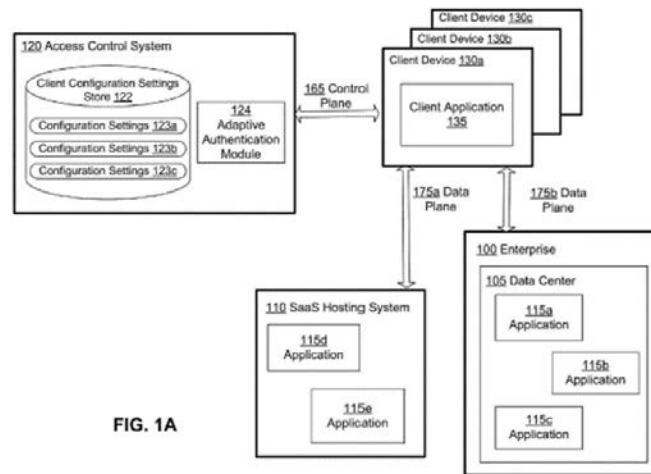


FIG. 1A

Figure 1A illustrates an environment comprising one or more enterprises 100, one or more software-as-a-service (SaaS) hosting systems 110, one or more access control systems 120, and a plurality of client devices 130. Ex. 1001, 2:34–44. Client devices 130 allow users to use applications 115 of enterprise 100 as well as SaaS applications 115. *Id.* Enterprise 100 allows users of client devices 130 to access applications 115 associated with enterprise 100. *Id.* at 2:45–46.

Applications 115 associated with enterprise 100 are hosted within data center 105 managed by enterprise 100. *Id.* at 2:61–63. Data center 105 includes a firewall to control access to applications 115 hosted by data center 105, wherein users associated with enterprise 100 use login credentials to access applications 115 in data center 105. *Id.* at 3:4–16.

Client device 130 executes client application 135 for communicating with enterprise 100 and SaaS hosting system 110 to access applications 115, wherein client application 135 authenticates access to a requested application by sending login credentials to data center 105 or SaaS hosting system 110. *Id.* at 3:32–52. Access control system 120 manages communications between client applications 135, enterprise 100, and SaaS

hosting system 110. *Id.* at 3:53–61. Access control system 120 is external to enterprise 100 and SaaS hosting system 110. *Id.*

When a user requests access to application 115, client application 135 sends the request to access control system 120, and access control system 120 determines an address of the requested application and a type of access control for client application 135 based on a context of the request. *Id.* at 4:10–27. Factors included in the context include the enterprise or company for which the device is being used. *Id.* Using security policies associated with enterprise 100 with which the user is associated, access control system 120 determines the type of access control required for the user to access the requested application. *Id.* The level of security applied to applications 115 varies depending on the context in which client application 135 is operated. *Id.* at 4:28–30. The administrator of enterprise 100 interacts with an admin tool 305 to define access control policies for enterprise 100. *Id.* at 7:50–58.

B. Illustrative Claim

Of the challenged claims, claims 1, 13, and 18 are independent. Claim 1 is illustrative of the claims at issue and is reproduced below:

1. A method comprising:
 - storing, by an access control system, action control policies for a plurality of enterprises, wherein the access control system is external to each of the plurality of enterprises;
 - storing, by the access control system, action control policies for the plurality of enterprises as a mapping from contexts of requests to the action control policies, each context specifying one or more attributes describing a request received from a client device, wherein the request is for an action performed by an application hosted by a software as a services (SaaS) hosting system, each action control policy identifying actions that the client device is allowed in a given context;

receiving, by the access control system, from a first client device, a first request for interacting with the application hosted by the SaaS hosting system, the first request providing information describing a first context;

identifying a first enterprise from the plurality of enterprises, the first enterprise associated with the first client device;

determining, by the access control system, a first action control policy associated with the first enterprise for the first context based on the mapping, the first action control policy allowing a first set of actions supported by the application;

sending information describing the first action control policy to the first client device for enforcement of the first action control policy by an agent executing on the first client device;

receiving from a second client device, a second request for interacting with the application hosted by the SaaS hosting system, the second request providing information describing a second context;

identifying a second enterprise from the plurality of enterprises, the second enterprise associated with the second client device;

determining a second action control policy associated with the second enterprise for the second context based on the mapping, the second action control policy allowing a second set of actions supported by the application; and

sending information describing the second action control policy to the second client device for enforcement of the second action control policy by the agent executing on the second client device.

Ex. 1001, 13:60–14:37.

C. Prior Art

Petitioner relies on the following references (*see* Pet. 1–2):

Reference or Declaration	Exhibit No.
U.S. Patent No. 8,869,235 B2 (October 21, 2014) (“Qureshi”)	1003
U.S. Patent No. 8,578,443 B2 (November 5, 2013) (“Narain”)	1004
U.S. Patent No. 8,713,633 B2 (April 29, 2014) (“Thomas”)	1005
U.S. Patent Publication No. 2012/0210068 A1 (August 16, 2012) (“Joshi”)	1006
U.S. Patent Publication No. 2006/0282876 A1 (December 14, 2006) (“Shelest”)	1007

Petitioner further relies on the declaration of its expert, Jon B. Weissman, Ph.D. (Ex. 1002). Dr. Weissman was cross-examined by Patent Owner, and a transcript of his deposition was entered into the record. Ex. 2003. Patent Owner provides a declaration by Jean-Philippe P. Labruyère. Ex. 2002. Mr. Labruyère was cross-examined by Petitioner, and a transcript of his deposition was entered into the record. Ex. 1010.

D. Asserted Grounds of Unpatentability

We instituted *inter parties* review on all claims and all grounds in the Petition. The Petition asserts that the challenged claims are unpatentable on the following grounds (*see* Pet. 1–2):

Claims Challenged	Basis	References
1–5, 7, 8, and 10–18	§ 103(a)	Qureshi
6	§ 103(a)	Qureshi, Joshi
9	§ 103(a)	Qureshi, Shelest
1–4, 7, 8, 10–16, and 18	§ 102(a)(2)	Narain
5 and 17	§ 103(a)	Narain, Thomas
6	§ 103(a)	Narain, Joshi
9	§ 103(a)	Narain, Shelest

II. ANALYSIS

A. Claim Construction

In an *inter partes* review proceeding, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent. 37 C.F.R. § 42.100(b).¹ Consistent with this standard, we assign claim terms their ordinary and customary meaning, as would be understood by one of ordinary skill in the art at the time of the invention, in the context of the entire patent disclosure. See *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

Petitioner proposes construction of the following claim language: “action control policies” and “attributes describing a request received from a client device.” Pet. 6–8. Petitioner contends its proposed constructions are consistent with the broadest reasonable interpretation standard. *Id.*

Patent Owner chooses not to address Petitioner’s proposed claim constructions but rather “submits that the challenged claims should be construed to require that the ‘receiving,’ ‘identifying,’ ‘determining,’ and ‘sending’ steps, recited in independent claims 1, 13, and 17, be performed in the sequence they are presented in the claim.” PO Resp. 7. In particular, Patent Owner contends that “grammar, logic and the specification all compel the conclusion that an order is required.” *Id.* at 9. According to Patent Owner, as set forth by the Federal Circuit, an order is required “as a matter

¹ This standard applies to *inter partes* reviews filed before November 13, 2018. 77 Fed. Reg. 48727 (Aug. 14, 2012) (codified at 37 C.F.R. § 42.100(b)), as amended at 81 Fed. Reg. 18766 (Apr. 1, 2016); see also 83 Fed. Reg. 51340 (Oct. 11, 2018) (changing the standard for interpreting claims in *inter partes* reviews filed on or after November 13, 2018).

of logic or grammar,” and/or when “the specification ‘directly or implicitly requires such a narrow construction.’” *Id.* (quoting *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369–70 (Fed. Cir. 2003)).

In its Reply, Petitioner contends that the “broadest reasonable interpretation of the claims” does not require the steps to occur in order. Reply 3–7. According to Petitioner, “Patent Owner improperly attempts to read limitations from the ’182 patent specification into the claims” when asserting that the steps must occur in order. *Id.* at 7.

Only terms that are in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)). For the reasons set forth below, the explicit requirements set forth in claims 1, 13, and 17 themselves sufficiently limit them claims without requiring Patent Owner’s proposed construction. We determine that we need not further construe expressly any claim terms to resolve the arguments before us.

B. Asserted Obviousness of the Claims over Qureshi

Petitioner contends that claims 1–5, 7, 8, and 10–18 would have been obvious over Qureshi; that claim 6 would have been obvious over Qureshi and Joshi; and claim 9 would have been obvious over Qureshi and Shelest. Pet. 13–42. Petitioner relies on the declaration of Dr. Weissman for support. *See* Ex. 1002 ¶¶ 120–196. Patent Owner disputes Petitioner’s contentions. PO Resp. 27–52. Patent Owner relies on the declaration of Mr. Labruyère for support. *See* Ex. 2002 ¶¶ 106–187.

1. *Principles of Law*

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 skill in the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations). *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We analyze these asserted grounds based on obviousness with the principles identified above in mind.

2. *Level of Skill in the Art*

The level of skill in the art is a factual determination that provides a primary guarantee of objectivity in an obviousness analysis. *Al-Site Corp. v. VSI Int’l Inc.*, 174 F.3d 1308, 1324 (Fed. Cir. 1999) (citing *Graham*, 383 U.S. at 17–18; *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991)). Dr. Weissman, asserts that a person having ordinary skill in the art at the time of the invention would have to be an individual with “either a bachelor’s degree in computer science, with at least three to four years of experience in remote accessed computer systems, or Master’s degree in computer science, with at least two years of experience in remote accessed computer systems.” Ex. 1002 ¶ 14. Patent Owner does not assess the level of ordinary skill in the art. *See generally* PO Resp.

We adopt Dr. Weissman's assessment of the level of ordinary skill in the art because it is consistent with the '182 patent and the asserted prior art, and apply it to our obviousness evaluation below. We also observe that the prior art of record reflects the level of ordinary skill in the art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

3. *Qureshi (Ex. 1003)*

Qureshi relates to a system for enabling enterprise users to securely access enterprise resources using mobile devices. Ex. 1003, code (54). The system implements policies for controlling mobile device accesses to enterprise resources based on device attributes, behavioral attributes, and other criteria. *Id.* at code (57).

Figure 1B of Qureshi is reproduced below:

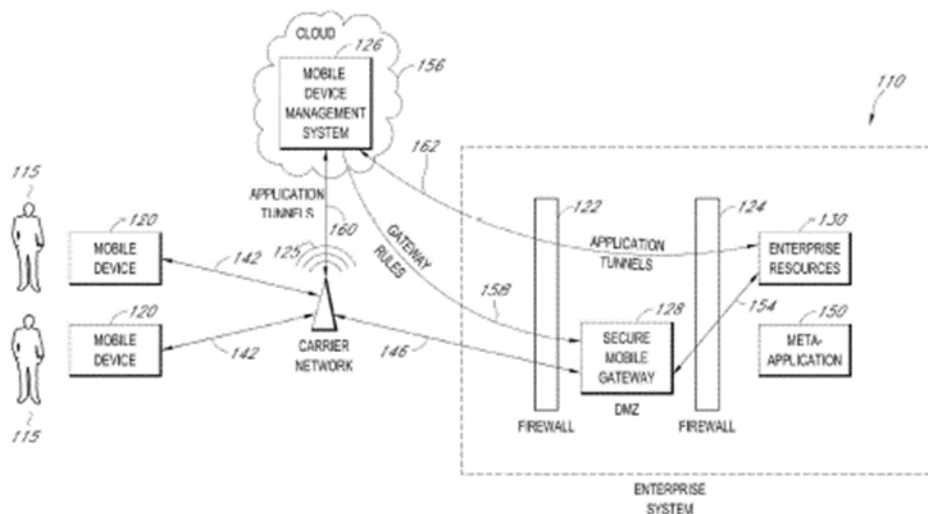


FIG. 1B

Figure 1B depicts a computer system 110 associated with an enterprise, and users 115 and mobile computing devices 120 associated therewith. Ex.

1003, 7:46–49. Mobile devices 120 are configured to communicate with enterprise system 110 over communication network 125. *Id.* at 7:53–55. Enterprise system 110 includes external firewall 122 and internal firewall 124, each firewall 122, 124 comprising one or more device designed to permit or deny network transmission based upon certain criteria. *Id.* at 7:64–67.

Enterprise system 110 includes secure mobile gateway 128. *Id.* at 8:25–28. Mobile device 120's enterprise access request is sent to secure mobile gateway 128, and gateway 128 sends the request to enterprise resource 130 via internal connection 154. *Id.* at 8:35–45. Mobile device management system 126 acts as a “tunneling mediator” within an application tunnel between mobile device 120 and enterprise resource 130. *Id.* at 8:49–54. Mobile device management system 126 and meta-application 150 are respectively located in cloud computing system 156. *Id.* at 8:55–59. Cloud-based device management system 126 is configured to provide gateway rules to secure mobile gateway 128 via connections 158. *Id.* at 9:7–12.

Device configuration information collected by an enterprise agent is reported to mobile device management system 126, which then uses the information to generate rules applied to secure mobile gateway 128 to control mobile device 120's accesses to enterprise resources 130. *Id.* at 11:67–12:6. Mobile device management system 126 includes enterprise access policies 218 stored in computer storage that defines conditions under which mobile device access to enterprise resources 130 will be granted or denied, wherein mobile device management system 126 uses access policies

218 to process mobile device access requests received by mobile device management system 126. *Id.* at 16:8–27.

Secure mobile gateway 128 assists in protecting sensitive enterprise data accessed by mobile devices 120, monitors and logs traffic between enterprise resources 130 and mobile device 120, applies rules to implement enterprise policies applied to selected mobile device 120, and takes actions to implement enterprise policies as applied to selected mobile device 120 that is requesting access to enterprise resource 130. *Id.* at 18:15–28. Secure mobile gateway 128 can be implemented to handle requests associated with two or more different enterprise systems 110, including systems 110 of distinct companies or enterprises. When handling requests associated with a plurality of different enterprise computing systems 110, secure mobile gateway 128 implements different rules for each of different enterprise computer systems 110. *Id.* at 19:33–42.

Secure mobile gateway 128 includes log redirector service 412 that periodically reads logged data 410 and sends it to analytic service 414. *Id.* at 78:4–8. The logged data can include data from mobile device access requests 402 received by gateway filter 401 of secure mobile gateway 128. *Id.* at 80:1–6. Analytics server 414 can employ a user determination algorithm for determining user information associated with request 2302 received by enterprise resource 130, wherein the user information can include a determination of whether request 2302 was sent by user 115 (as opposed to someone who is not associated or enrolled with the enterprise), a determination of whether user 115 identified in user determination request 2304 is the person who sent request 2302 to the enterprise resource 130,

and/or an identification (e.g., username) of user 115 who sent request 2302. *Id.* at 80:30–40.

Mobile device management system 126 includes storage repository 212 storing a plurality of different mobile device rules 214. *Id.* at 52:52–55. The repository also includes remedial actions 216 for countering problems, wherein mobile device rules 214 and their associated remedial actions are organized into separate “rule packages.” *Id.* at 53:50–54:1. Mobile device manager 202 is preferably responsible for sending appropriate rule packages to mobile devices 120 based on properties 208 of the mobile devices and rules of the users assigned to the mobile devices. *Id.* at 54:39–43. In an embodiment, mobile device manager 202 is configured to use a new user’s role information and/or mobile device properties to determine an appropriate mobile device rule package to send to the user’s mobile device 120. *Id.* at 55:5–9.

4. *Claims 1–18*

Petitioner asserts that Qureshi teaches and suggests “storing, by an access control system, action control policies for a plurality of enterprises,” wherein “the access control system is external to each of the plurality of enterprises.” Pet. 15–20. Petitioner also asserts that Qureshi teaches and suggests the recited “receiving,” “identifying,” “determining,” and “sending” steps. *Id.* at 24–28.

- a. *“storing, by the access control system, action control policies for the plurality of enterprises” (claims 1, 13, and 18)*

According to Petitioner, Qureshi teaches “a mobile device management system 126 (‘access control system’) storing mobile device rules 214 (‘action control policies’).” Pet. 15 (citing Ex. 1003, 52:52–55;

Ex. 1002 ¶ 54). Petitioner contends Qureshi teaches that the mobile device management system can be located in cloud 156 “external to the enterprise 110.” *Id.* at 19 (citing Ex. 1003, 1:49–51, Fig. 1B; Ex. 1002 ¶ 65).

Although Petitioner acknowledges that “Qureshi does not explicitly teach that the mobile device management system (‘access control system’) stores rules for a plurality of enterprises,” Petitioner contends Qureshi discloses that a different component, “the secure mobile gateway 128 ‘can be implemented to handle requests associated with **two or more different enterprise systems 110.**’” *Id.* at 17 (quoting Ex. 1003, 19:35–48; Ex. 1002 ¶ 59). Petitioner contends that, in view of Qureshi’s secure mobile gateway 128 handling requests associated with a plurality of enterprises, it would have been obvious for Qureshi’s mobile device management system to store rules for a plurality of enterprises. *Id.* at 17–19 (citing Ex. 1002 ¶¶ 61–64).

Petitioner asserts that “it would have been obvious to modify Qureshi to support multiple enterprises because doing so would have involved application of a known technique to a system ready for improvement, with the predictable result of reducing complexity and cost.” Reply 19 (citing Pet. 15–19). According to Petitioner, “a skilled artisan would have understood the benefits of sharing a mobile device management system among enterprises.” *Id.* at 21 (citing Pet. 15–19). Citing its expert, Petitioner contends “that moving the mobile device management system into the cloud, where it can be shared [among] multiple enterprises, would reduce the cost of IT staff for the different enterprises.” *Id.* (citing Ex. 2003, 69:2–70:7).

Patent Owner contends that Qureshi explicitly teaches that “each enterprise sharing the secure mobile gateway 128 would still have its own

separate mobile device management system 126,” because Qureshi desires “a single enterprise having multiple mobile device management systems 126 for different office locations.” PO Resp. 42–43 (citing Ex. 1003, 17:4–22, 19:45–48; Ex. 2002 ¶¶ 160–161). Patent Owner’s expert, Mr. Labruyère, opines that “a person of ordinary skill in the art would understand that it would be beneficial to have multiple mobile device management systems 126 for a single enterprise [instead of a single mobile device management systems 126 for a plurality of enterprises] for a number of reasons”: 1) “improve the overall performance of the enterprise system for example, by reducing latency”; 2) “address scalability limitations of each individual mobile device management system”; 3) “aid the enterprise in complying with different data management standards or laws imposed by different geographical regions or countries”; and 4) “maintain some level of isolation by having each enterprise maintain its own mobile device management system” to “mitigate . . . risk” to “the integrity of the enterprise’s security.” Ex. 2002 ¶¶ 162–165.

Petitioner responds that “[t]he plain language of Qureshi simply states that **different** (e.g., two) enterprises **could** have different mobile device management system in some embodiments,” and that Qureshi “says nothing about whether **every** enterprise **would** have its own mobile device management system.” Reply 20 (citing Ex. 1003, 19:45–48). Petitioner argues that, instead, “a skilled artisan would have understood the benefits of sharing a mobile device management system among enterprises” (*id.* at 21 (citing Pet. 15–19)), citing Dr. Weissman’s testimony “that moving the mobile device management system into the cloud, where it can be shared

[among] multiple enterprises, would reduce the cost of IT staff for the different enterprises.” Reply 21 (citing Ex. 2003, 69:2–70:7).

According to Patent Owner, however, merely relocating the mobile device management system outside of the single enterprise and into the cloud to be shared by a plurality of enterprises does not address its expert’s opinion that such a move would require security to mitigate risk. Sur-Reply 15–16 (citing Ex. 2002 ¶¶ 171–72). We agree.

Although “[a] person of ordinary skill in the art is also a person of ordinary creativity, not an automaton,” *KSR*, 550 U.S. at 421, there may be limits in a particular case as to how much gap-filling may be based on such creativity. See *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361 (Fed. Cir. 2016); *DSS Tech. Mgmt., Inc. v. Apple Inc.*, 885 F.3d 1367, 1374–75 (Fed. Cir. 2018) (reliance on ordinary creativity to supply a missing limitation requires same “searching” inquiry as reliance on common sense).

Here, we find that Petitioner has not met its burden to prove that one of ordinary skill in the art would have understood Qureshi to teach or suggest that “the mobile device management system 126 stores action control policies for a plurality of enterprises.” PO Resp. 41–42; Ex. 2002 ¶¶ 155, 157–160, 167. Specifically, we agree with Patent Owner that Petitioner fails to provide persuasive evidence that one of ordinary skill in the art would have found it obvious “for Qureshi’s mobile device management to store rules for a plurality of enterprises as taught by Qureshi’s secure mobile gateway.” Pet. 17. Although Qureshi teaches secure mobile gateway 128 may handle more than one enterprise system, that component is not the alleged access control system of claim 1. Instead, Petitioner relies solely on Dr. Weissman’s testimony to support its

conclusion that it would have been obvious to share the mobile device management system among a plurality of enterprises.

We find the testimony of Dr. Weissman insufficient to support Petitioner's position. Ex. 2003, 62:22–65:11. In his declaration, Dr. Weissman testified that, in Qureshi, “[t]he secure mobile gateway 128 can include a gateway configuration service 406 that allows a user . . . to view, edit and/or create gateway rules 404, and ***then save them in the local database,***” wherein the gateway rules “are used by a ***secure mobile gateway to grant and deny mobile device requests to access enterprise resource.***” Ex. 1002 ¶¶ 60–61 (quoting Ex. 1003, 23:48–51, 6:30–33). However, such reference to Qureshi is directed to internally-located secure mobile gateway 128 storing rules for granting access to the enterprise resource for the mobile devices, but does not explain how Qureshi teaches storing “action control policies” for “a plurality of enterprises” externally to the enterprises. Nor does Dr. Weissman provide a persuasive explanation supported by evidence in the record for concluding that the claimed action control policies for a plurality of enterprises would be stored by the mobile device management 126 or any device in a cloud. *See id.*

In its Reply, Petitioner presents a new argument that “Qureshi unequivocally discloses that the ‘Use of Mobile Device Management System to Regulate Mobile Device Access to Enterprise System,’ ‘Authentication of Mobile Device Users,’ and ‘Device-Resident Management System’ features can be implemented within a single system,” wherein “the ‘Device-Resident Management System’ feature is implemented using device management system 126, which is part of system 110” while “the ‘Authentication of Mobile Device User’ feature is implemented using secure mobile gateway

128, which is also part of system 110.” Reply 16–17. That is, Petitioner’s new position appears to be that Qureshi’s mobile device management system comprises secure mobile gateway 128 as well as mobile device management system 126. *Id.*

However, during his cross-examination testimony, when presented with the hypothetical in which “the secure mobile gateway 128 is moved into the cloud and multiple enterprises are accessing the mobile gateway 128,” Dr. Weissman testified that he is “not certain” whether “there [would] still be multiple firewalls between the mobile gateway and the different enterprises’ resources.” Ex. 2003, 62:17–63:6. According to Dr. Weissman, “[t]he security mobile gateway, if it’s implemented in the cloud, would have to have sufficient isolation between the different enterprise resources, different enterprises,” wherein “security technology exists to do that,” but Dr. Weissman testified “I have no idea of the cost distinction there” and acknowledged “[i]t’s always possible [that the system could be slower].” *Id.* at 63:15–22, 64:12–16, 65:11. Because Dr. Weissman insufficiently explains why one of ordinary skill in the art would move secure mobile gateway 128 to a cloud and then store action control policies in a secure mobile gateway located in the cloud we give this testimony less weight.

Patent Owner’s expert, Mr. Labruyère, identifies these deficiencies in Petitioner’s reasoning, including addressing Petitioner’s theory that it would have been obvious to modify Qureshi’s mobile device management system 126 to store action control policies for a plurality of enterprises. Ex. 2002 ¶¶ 153–177. In particular, “the secure mobile gateway 128 is an enterprise resource that is designed to prevent unauthorized access to enterprise resources”; thus, “[u]sing one secure mobile gateway 128 for multiple,

distinct enterprises would threaten the integrity of each individual enterprise's security.” *Id.*

In sum, based on our review of the record, we find Petitioner's showing is insufficient. In evaluating whether Petitioner adequately shows that one of skill in the art would move the secure mobile gateway 128 to the cloud, the evidence supports Mr. Labruyère's opinion that using a single secure mobile gateway to communicate with different enterprises “would be unusual” wherein such modification could “threaten the integrity of each individual enterprise's security.” Ex. 2002 ¶ 157.

b. The “receiving” and “identifying” steps (claims 1, 13, and 18)

Petitioner also does not persuasively show that Qureshi teaches or suggests the steps of “receiving” and “identifying” as claimed.

Petitioner contends Qureshi discloses that “mobile devices 120 can be configured to send device-related data to the mobile device management system 126,” and thus, “Qureshi teaches that the mobile device management system receives from a mobile device a request for interacting with an application.” Pet. 24 (citing Ex. 1003, 15:63–16:1 (emphasis omitted); Ex. 1002 ¶ 73). According to Petitioner, Qureshi teaches “the first request providing information describing a first context” since “Qureshi discloses using information in the request header or body to determine information about the user and/or device associated with the device (i.e., context).” *Id.* at 24–25 (citing Ex. 1003, 44:30–34, Fig. 2; Ex. 1002 ¶ 75).

Petitioner then contends Qureshi's “secure mobile gateway 128 can be implemented to handle requests associated with two or more different enterprise systems 110.” Pet. 25 (quoting Ex. 1003, 19:36–38 (emphasis omitted)). Thus, according to Petitioner, Qureshi teaches “identifying if a

mobile device user is associated with a particular (‘first’) enterprise” because, in Qureshi, “analytics service 414 can employ a user determination algorithm for determining user information associated with the request 2302” and “whether the request 2302 was sent by a user 115 (as opposed to someone who is not associated or enrolled with the enterprise).” *Id.* (citing Ex. 1003, 80:30–36; Ex. 1002 ¶ 77 (emphasis omitted)).

In its Reply, Petitioner asserts that, “given that it would have been obvious for Qureshi to provide access control for a plurality of enterprises, Qureshi *would have identified an enterprise from a plurality of enterprises.*” Reply 12 (emphasis added). According to Petitioner, “analytic service 414 would have to determine whether a request was sent by a first user associated with a first enterprise (‘as opposed to someone who is not associated or enrolled with the enterprise’) or if the request was sent by a second user associated with a second enterprise.” *Id.* at 13 (quoting Ex. 1003, 80:30–36).

Based on the record before us, and given that the step of identifying a first enterprise refers back to the “first client device” introduced in the receiving step, Petitioner does not persuasively show that Qureshi teaches or suggests “identifying a first enterprise from a plurality of enterprises,” wherein the first enterprise is “associated with the first client device” from which the access control system receives “a first request for interacting with the application.” Ex. 1001, 14:6–13.

In Qureshi’s enterprise system 110, mobile device 120 sends an enterprise access request to secure mobile gateway 128, and secure mobile gateway 128 sends the request to enterprise resource 130. Ex. 1003, 8:25–9:12, 11:67–12:6. When handling requests associated with a plurality of

different enterprise computing systems 110, secure mobile gateway 128 implements different rules for each of different enterprise computer systems 110. *Id.* at 19:33–42. Analytics server 414 employs a user determination algorithm for determining user information associated with the request, the user information including a determination of whether the request was sent by a user (as opposed to someone who is not associated or enrolled with the enterprise), a determination of whether the user identified in the user determination request is the person who sent the request to the enterprise resource 130, and/or an identification (e.g., username) of the user who sent the request. *Id.* at 80:30–40.

Although Petitioner contends that “analytic service 414 would have to determine whether a request was sent by a first user associated with a first enterprise (‘as opposed to someone who is not associated or enrolled with the enterprise’)” (Reply 13 (citing Ex. 1003, 80:30–36)), Patent Owner points out that “[a] person of ordinary skill in the art would understand that the cited portion of Qureshi regarding user authentication simply refers to verifying that a user making a request *is a recognized user* based on their provided credentials.” PO Resp. 33 (emphasis added) (citing Ex. 2002 ¶ 125). According to Mr. Labruyère, “[a] person of ordinary skill in the art understands that authentication of a user refers to verifying that a user or device making a request is a recognized user or device based on their credentials,” as consistent with Qureshi, in which “the analytics services 414 is essentially being asked to verify whether the identified user 115 is the actual person who sent the request 2302.” Ex. 2002 ¶¶ 125–126 (citing Ex. 1003, 80:27–29). That is, a person of ordinary skill in the art would have understood that “Qureshi’s authentication process is not determining

whether the user or mobile device is associated with enterprise A, enterprise B, or enterprise C.” *Id.* ¶ 127.

Petitioner contends that Patent Owner and its expert “fail to address Petitioner’s contention that . . . Qureshi would have identified an enterprise from a plurality of enterprises.” Reply 12 (citing PO Resp. 32–35; Ex. 2002 ¶¶ 50–55). We disagree. Petitioner’s contention is based solely on Dr. Weissman’s testimony. Pet. 25 (citing Ex. 1002 ¶ 77). Dr. Weissman’s statement that Qureshi teaches “identifying if a mobile device user is associated with a particular [first] enterprise” is based on Qureshi’s determining “whether the request 2302 was sent by a user 115 (as opposed to someone who is not associated or enrolled with the enterprise).” Ex. 1002 ¶ 77 (citing Ex. 1003, 80:30–36).

As Mr. Labruyère asserts, however, “enterprise resource 130 is part of the enterprise,” and thus, “there is no need to determine which one of several enterprises the user or mobile device is associated with.” Ex. 2002 ¶ 128. According to Mr. Labruyère, “[a] person of ordinary skill in the art would understand that when Qureshi refers to ‘someone who is not associated or enrolled with the enterprise,’ it is referring to someone failing to provide the proper credentials to access the enterprise resource 130.” *Id.* ¶ 129 (citing Ex. 1003, 80:34–35). That is, as the ’182 Specification demonstrates, there are “differences between identifying an enterprise from a plurality of enterprises and authenticating a user or mobile device.” *Id.* ¶ 130. We agree. Accordingly, we give more weight to Mr. Labruyère’s testimony.

Based on our review of the record, we find Petitioner’s showing is insufficient. The evidence supports Mr. Labruyère’s opinion that, since “enterprise resource 130 is part of the enterprise,” “there is no need to

determine which one of several enterprises the user or mobile device is associated with,” wherein there are “differences between identifying an enterprise from a plurality of enterprises and authenticating a user or mobile device.” Ex. 2002 ¶¶ 128–130.

c. The “determining” and “sending” steps (claims 1, 13, and 18)

Petitioner contends that Qureshi teaches or suggests the “determining” and “sending” steps. In particular, Petitioner contends that Qureshi’s “mobile device management system determines a mobile device rule (‘first action control policy’) based on the mapping from the context of a request (e.g., mobile device properties) to the rule.” Pet. 26 (citing Ex. 1003, 54:39–43); Ex. 1002 ¶ 79. According to Petitioner, Qureshi’s mobile device rule is associated with an enterprise. Pet. 26 (“[A] rule package of mobile device rules . . . can be prepared for all users 115 having roles 206 that that are sales-oriented (e.g., all sales people of the enterprise)” (quoting Ex. 1003, 54:6–9)); Ex. 1002 ¶ 80. Furthermore, according to Petitioner, “Qureshi teaches sending the mobile device rule (‘first action control policy’) to the mobile device.” Pet. 28 (citing Ex. 1003, 54:39–43 (“mobile device manager 202 is preferably responsible for sending appropriate rule packages to the mobile devices 120”)); Ex. 1002 ¶ 84.

Based on the record before us, Petitioner does not persuasively show that Qureshi teaches or suggests “sending information describing the first action control policy to the first client device for enforcement of the first action control policy,” wherein the first action control policy is determined as being “associated with the first enterprise for the first context based on the mapping,” as required by the “determining” step, and wherein the first

context is described in information provided in the first request, as required by the “receiving” step. Ex. 1001, 14:14–22.

In Qureshi’s method of regulating mobile device access, mobile device management system 126 receives an access request from a mobile device, and in response, tunnel mediator 224 determines whether one or more properties of mobile device 120 comply with one or more relevant access policies 218. Ex. 1003, 44:50–61. Next, the method includes determining whether one or more properties of user 115 assigned to mobile device 120 are in compliance with one or more relevant access policies 218, and thereafter, tunneling mediator 224 of mobile device management system 126 either grants access or denies access. *Id.* at 45:4–19.

Mobile device management system 126 also includes storage repository 212 storing a plurality of different mobile device rules 214 and remedial actions 216 organized into separate “rule packages.” Ex. 1003, 52:52–55, 53:50–54:1. Mobile device manager 202 sends appropriate rule packages to mobile devices 120 based on properties of the mobile devices and rules of the users assigned to the mobile devices. *Id.* at 55:5–9.

We find Petitioner’s statement that “mobile device manager 202 is preferably responsible for sending appropriate rule packages to the mobile device” (Ex. 1003, 54:39–43) to be insufficient support that Qureshi teaches or suggests “sending information describing the first action control policy to the first client device,” wherein the first action control policy “associated with the first enterprise for the first context,” but wherein the first context is described in information provided in a request sent for interaction with the program, as claimed. Pet. 37; Ex. 1001, 14:14–22.

As Patent Owner points out, “[a]t best, this embodiment merely describes mobile device rules 214 being sent to the mobile device 120 as part of an initial provisioning of the device or responsive to a policy update from the enterprise.” PO Resp. 39 (citing Ex. 2002 ¶¶ 139, 143). That is, this embodiment describes sending mobile device rules 214 to mobile device 120, not any action control policy determined as being associated with an enterprise for a context described in information provided in a request for interaction with a program, as required by the claims.

In Qureshi, access policies 218, not mobile device rules 214, are determined as being associated with a context described in a request for interaction with a program. Ex. 1003, 44:50–61. Patent Owner points to the testimony of Dr. Weissman, in which he “agrees that sending rules packages [comprising mobile device rules 214 and remedial actions 216] to the mobile device 120 ‘occurs elsewhere’ in Qureshi.” PO Resp. 31 (citing Ex. 2003, 48:12–23). As Patent Owner asserts, Qureshi “does not disclose sending the access policies 218 to the mobile device 120.” *Id.* (citing Ex. 1003, Fig. 7; Ex. 2002 ¶ 118). Instead, according to Patent Owner, in Qureshi, “determining compliance with access policies 218 is binary (i.e., yes or no).” *Id.* (citing Ex. 2002 ¶ 117). In determining compliance with access policies 218, there is no sending of the policies to mobile device 120. *Id.*

The testimony of Mr. Labruyère is consistent in identifying these deficiencies in Qureshi and it is therefore entitled to more weight. Ex. 2002 ¶¶ 133–143. In particular, Mr. Labruyère testified that the embodiment in Qureshi relied upon by Petitioner “merely describes rules packages being sent to the mobile device 120 as part of an initial provisioning of the device or responsive to a policy update from the enterprise.” *Id.* ¶ 143. That is, the

embodiment “fails to disclose that the rules packages are determined and sent to the mobile device 120 after the mobile device management system 126 receives a request for interacting with an application.” *Id.* ¶ 142.

Based on our review of the record, we find that Petitioner’s showing is insufficient, with the evidence instead supporting Patent Owner and Mr. Labruyère’s assessment that Qureshi does not teach or suggest the “determining” and “sending” steps as claimed. Petitioner has not provided evidence or persuasive reasoning for us to find differently.

Accordingly, for all the foregoing reasons, we conclude that Petitioner does not demonstrate, by a preponderance of the evidence, that independent claim 1 and independent claims 13 and 18, reciting similar limitations, are unpatentable under 35 U.S.C. § 103(a) over Qureshi. We similarly conclude, by virtue of the dependence of claims 2–12 and 14–17 respectively from claims 1 and 13, that Petitioner also does not demonstrate, by a preponderance of the evidence that: claims 2–5, 7, 8, 10–12, and 14–17 would have been obvious over Qureshi; claim 6 would have been obvious over Qureshi and Joshi; or claim 9 would have been obvious over Qureshi and Shelest.

C. Asserted Anticipation by and Obviousness of the Claims over Narain

Petitioner contends that claims 1–4, 7, 8, 10–16, and 18 are anticipated by Narain; that claims 5 and 17 would have been obvious over Narain and Thomas; that claim 6 would have been obvious over Narain and Joshi; and that claim 9 would have been obvious over Narain and Shelest. Pet. 42–64. Petitioner relies on the declaration of Dr. Weissman for support. *See* Ex. 1002 ¶¶ 132–194. Patent Owner disputes Petitioner’s contentions.

PO Resp. 52–60. Patent Owner relies on the declaration of Mr. Labruyère for support. *See* Ex. 2002 ¶¶ 188–215. We provide a brief description of Narain before turning to the parties’ contentions.

1. *Narain (Ex. 1004)*

Narain relates to a method of mobile device management that includes routing communications between the mobile device and a network cloud through an enforcement engine and generating a policy regarding the mobile applications such that compliance of the mobile device with the policy is enforced in real time. Ex. 1004, Abstract.

Figure 1B of Narain is reproduced below:

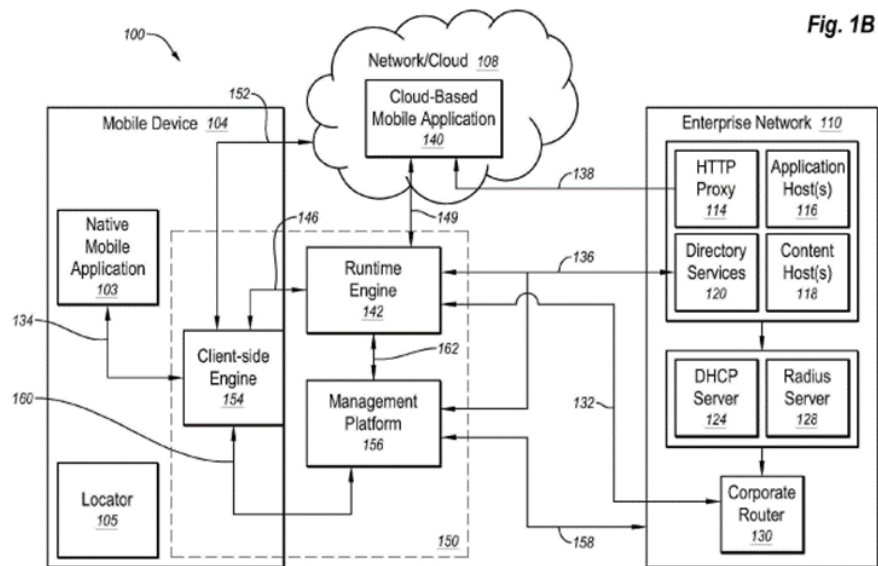


Figure 1B depicts an operating environment 100 including mobile device 104, public network and/or cloud 108, and enterprise network 110. *Id.* at 5:36–44. Mobile application management policy enforcement engine 150 is included in a mobile application management system in operating environment 100, wherein enforcement engine 150 manages mobile applications on mobile device 104. *Id.* at 5:44–50. Although Figure 1B depicts one mobile device 104, there may be multiple mobile devices 104 in

operating environment 100. *Id.* a 5:58–60. Enforcement engine 150 is customized to operating environment 100 through the generation of a policy that may include specific controls and/or security features/protocols specific to operating environment 100. *Id.* at 7:48–59. The policy may include provisions for a first user to use a first private mobile application and a second user to use a second private mobile application, wherein the first user and/or the second user may include individuals, an enterprise group, or the enterprise itself. *Id.* at 19:11–18.

2. Claims 1–18

As discussed above with respect to Qureshi, claim 1 recites, in relevant part, “storing, by an access control system, action control policies for a plurality of enterprises,” “wherein the access control system is external to each of the plurality of enterprises,” and “identifying a first[/second] enterprise from the plurality of enterprises, the first[/second] enterprise associated with the first[/second] client device.” Claims 13 and 18 recite similar limitations.

According to Petitioner, “Narain teaches an access control system storing policies for a plurality of enterprises” because Narain discloses “an enforcement engine 150 (‘access control system’) that includes ‘a client-side enforcement engine (client-side engine) 154, a runtime enforcement engine (runtime engine) 142, and a management platform 156 that in some combination **enforce compliance with the policy.**’” Pet. 43 (quoting Ex. 1004, 8:30–33). Further, according to Petitioner, “the management platform 156 ‘may accommodate a multi-tenant system in which **each tenant represents an enterprise customer 160A,**’” and “the pooling module 228, which is part of the management platform 156, ‘may centrally **store**

information related to the policy.” Pet. 43 (quoting Ex. 1004, 13:64–65, Fig. 2; Ex. 1002 ¶ 133). Furthermore, Petitioner contends Narain teaches “wherein the access control system is external to each of the plurality of enterprises,” because Narain shows “runtime engine 142 and management platform 165 external to enterprise network 110.” *Id.* at 44 (citing Ex. 1004, Fig. 1B; Ex. 1002 ¶ 135).

Petitioner then contends that “Narain teaches identifying an enterprise associated with a mobile device” because “Narain discloses that a policy may apply to a set of users” wherein “a ‘user’ may correspond to an enterprise and, thus, a policy may apply to a particular enterprise.” *Id.* at 47–48 (citing Ex. 1004, 19:1–7, 15–17).

Based on the record before us, Petitioner does not demonstrate, by a preponderance of the evidence, that Narain teaches or suggests “identifying a first[/second] enterprise from the plurality of enterprises, the first[/second] enterprise associated with the first[/second] client device,” as claimed in claim 1.

“[A] prior art reference—in order to anticipate under 35 U.S.C. § 102—must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements ‘arranged as in the claim.’” *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008) (citation omitted).

Here, Patent Owner has put forward persuasive evidence and argument that Narain is directed to identifying a user of an enterprise, wherein “the ‘182 patent makes clear that identifying an enterprise from a plurality of enterprises is not the same as identifying a user.” PO Resp. 53; *see* Ex. 1001, 6:19–20 (making the distinction between “an identifier of a

user” and “an identifier of the client device 130”), 8:20–23 (distinguishing between a “context” and a “user identifier”), 4:17–20 (“context” can include “enterprise or company for which the device is being used”). As Patent Owner points out, the Petition “does not separately address the requirements of [identifying a first enterprise and] identifying a second enterprise” from a plurality of enterprises. *Id.* at 53–54.

Instead, Petitioner maps Narain’s “enterprise network 110” to the claimed “enterprise,” while contending that Narain teaches “storing, by an access control system, action control policies for a plurality of enterprises,” “wherein the access control system is external to each of the plurality of enterprises.” Pet. 43–44 (citing Ex. 1004, Fig. 1B). However, Petitioner goes on to map Narain’s “users” to the claimed “enterprise” in contending that “Narain discloses that a policy may apply to a set of users” wherein “a ‘user’ may correspond to an enterprise and, thus, a policy may apply to a particular enterprise.” *Id.* at 47–48 (citing Ex. 1004, 19:1–7, 15–17). In other words, under Petitioner’s analysis, the claimed “enterprise” is Narain’s “enterprise network 110” but also a “user” that “may correspond to an enterprise.” *Id.* at 44, 47. Accordingly, Petitioner has not provided persuasive evidence or reasoning that Narain anticipates claims 1, 13, and 18.

In its Reply, Petitioner adds that “Narain uses a bottom up process,” wherein “Narain traverses up the enterprise sub-tree 170 to which the user belongs, until it reaches the user’s enterprise 160,” and thus, “Narain identifies the enterprise for each user request.” Reply 27–28. As an initial matter, as Patent Owner points out, “[t]he Petition did not rely on the so-called ‘bottom up process’ . . . for purportedly teaching the claimed

identification step,” and thus, Petitioner exceeds the proper scope of a Reply. Sur-Reply 21; *see* 37 C.F.R. § 42.23(b).

Nevertheless, we do not find this new argument persuasive. As Patent Owner also points out, Narain’s movement between levels of the substructures “is confined to an individual enterprise,” and as Patent Owner contends, identifying a user in a particular enterprise “is not equivalent to identifying an enterprise from a plurality of enterprises.” Sur-Reply 22 (citing Ex. 1004, Fig. 1A, 5:1–8 (describing the tree structure as departments within a single enterprise)).

Contrary to Petitioner’s assertion (Reply 27–28), the evidence supports Patent Owner’s assertion that Narain does *not* disclose the “identifying” step for identifying an enterprise “from the plurality of enterprises,” as claimed. As discussed above with respect to Qureshi, we agree with Mr. Labruyère that there are differences between identifying an enterprise from a plurality of enterprises and identifying a user. Ex. 2002 ¶ 130.

Accordingly, we conclude that Petitioner does not demonstrate, by a preponderance of the evidence, that independent claim 1 and independent claims 13 and 18, reciting similar limitations, are anticipated under 35 U.S.C. § 102(b) over Narain. We similarly conclude, by virtue of the dependence of claims 2–12 and 14–17 respectively from claims 1 and 13 that Petitioner also does not demonstrate, by a preponderance of the evidence, that: claims 2–4, 7, 8, 10–12, and 14–16 are anticipated by Narain; claims 5 and 17 would have been obvious over Narain and Thomas; claim 6 would have been obvious over Narain and Joshi; or claim 9 would have been obvious over Narain and Shelest.

III. ORDER

It is

ORDERED that, based on a preponderance of the evidence, claims 1–18 of U.S. Patent No. 9,426,182 B1 have not been shown to be unpatentable; and

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

In summary:

Reference(s)	Basis	Claims	Claims Shown Unpatentable	Claims Not Shown Unpatentable
Qureshi	§ 103(a)	1–5, 7, 8, 10–18	–	1–5, 7, 8, 10–18
Qureshi and Joshi	§ 103(a)	6	–	6
Qureshi and Shelest	§ 103(a)	9	–	9
Narain	§ 102(a)(2)	1–4, 7, 8, 10–16, 18	–	1–4, 7, 8, 10–16, 18
Narain and Thomas	§ 103(a)	5, 17	–	5, 17
Narain and Joshi	§ 103(a)	6	–	6
Narain and Shelest	§ 103(a)	9	–	9
Overall Outcome			–	1–18

IPR2018-00917
Patent 9,426,182 B1

PETITIONER:

Larissa Park
Kristoffer Lange
DLA PIPER LLP
larissa.bifano@dlapiper.com
kris.lange@dlapiper.com

PATENT OWNER:

Jennifer Hayes
Matthew Werber
Wayne Tang
NIXON PEABODY, LLP
jenhayes@nixonpeabody.com
mwerber@nixonpeabody.com
Wtang@nixonpeabody.com