

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-01010
Patent 8,843,643 B2

Before KARL D. EASTHOM, ROBERT J. WEINSCHENK, and
BETH Z. SHAW, *Administrative Patent Judges*.

WEINSCHENK, *Administrative Patent Judge*.

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

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–9, 12–24, and 27–32 of U.S. Patent No. 8,843,643 B2 (Ex. 1001, “the ’643 patent”). VirnetX Inc. (“Patent Owner”) filed a Preliminary Response (Paper 6, “Prelim. Resp.”) to the Petition. On October 29, 2015, we instituted an *inter partes* review of claims 1–9, 12–24, and 27–32 (“the challenged claims”) of the ’643 patent on the following grounds:

Claim(s)	Statutory Basis	Applied Reference(s)
1–8, 12–23, and 27–32	35 U.S.C. § 103(a)	Nancy J. Yeager & Robert E. McGrath, <i>Web Server Technology: The Advanced Guide for World Wide Web Information Providers</i> (Michael B. Morgan et al. eds., 1st ed. 1996) (Ex. 1008, “Yeager”); and Microsoft Internet Explorer 5 Resource Kit (1999) (Ex. 1006, “IE5 Resource Kit”)
9 and 24	35 U.S.C. § 103(a)	Yeager; IE5 Resource Kit; and Network Working Group, Request for Comments: 1034 (Nov. 1987) (Ex. 1024, “RFC 1034”)

Paper 9 (“Dec. on Inst.”), 14.

After institution, Patent Owner filed a Response (Paper 15, “PO Resp.”) to the Petition, and Petitioner filed a Reply (Paper 23, “Pet. Reply”) to the Response. An oral hearing was held on July 19, 2016, and a transcript of the hearing is included in the record. Paper 32 (“Tr.”).

We issue this Final Written Decision pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons set forth below, Petitioner has not

shown by a preponderance of the evidence that claims 1–9, 12–24, and 27–32 of the ’643 patent are unpatentable.

A. *Related Proceedings*

The parties indicate that the Petition in this case is related to the petition for *inter partes* review in IPR2015-01009, which also involves the ’643 patent. Pet. 2; Paper 5, 2. Patent Owner indicates that certain patents related to the ’643 patent are at issue in various *inter partes* reviews, reexaminations, and district court cases. Paper 5, 2–12.

B. *The ’643 Patent*

The ’643 patent relates to, *inter alia*, establishing a secure communication link between a computer and a server without a user of the computer having to enter any identification information, passwords, or encryption keys. Ex. 1001, col. 48, l. 66–col. 49, l. 1, col. 50, ll. 9–16. For example, a user of a computer may connect to a non-secure server by entering a domain name for the non-secure server in a Web browser. *Id.* at col. 49, ll. 21–32. The user then can enable a secure communication mode simply by clicking a “go secure” hyperlink in the Web browser. *Id.* at col. 50, ll. 9–12. The ’643 patent explains that a software module on the computer automatically replaces the domain name for the non-secure server with a secure domain name. *Id.* at col. 50, ll. 22–25. The software module then sends a query using the secure domain name to a secure domain name service (“SDNS”). *Id.* at col. 50, ll. 49–53. In response to the query, the SDNS returns an address for a secure server. *Id.* at col. 51, ll. 39–42. The computer then accesses the secure server through a virtual private network (“VPN”) communication link. *Id.* at col. 51, ll. 57–59.

C. *Illustrative Claim*

Claims 1 and 17 are independent. Claim 1 is reproduced below.

1. A method for establishing an encrypted communication link between a first device and a second device over a communication network, the method comprising:

enabling, at the first device, a secure communication mode without a user entering any cryptographic information for establishing the secure communication mode; and

establishing, based on a determination that the secure communication mode has been enabled, the encrypted communication link between the first device and the second device over the communication network, the establishing including:

constructing a domain name based on an identifier associated with the second device;

sending a query using the domain name;

receiving, in response to the query, at least one network address associated with the domain name; and

initiating establishment of the encrypted communication link between the first device and the second device over the communication network using the at least one network address and encrypted communication link resources received from a server that is separate from the first device.

Ex. 1001, col. 55, ll. 46–67.

II. ANALYSIS

A. *Claim Construction*

The claims of an unexpired patent are interpreted using the broadest reasonable interpretation in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–45 (2016). The parties propose construing several claim terms in the '643 patent. Pet. 9–15; PO Resp. 4–32. For the reasons

discussed below, we determine that no claim terms require express construction to resolve the parties' disputes regarding the asserted grounds of unpatentability in this case. *See infra* Sections II.B–II.C; *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.”).

B. *Obviousness of Claims 1–8, 12–23, and 27–32 Over Yeager and IE5 Resource Kit*

Petitioner argues that claims 1–8, 12–23, and 27–32 would have been obvious over Yeager and IE5 Resource Kit. Pet. 3. A claim is unpatentable as obvious under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the 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) any objective indicia of non-obviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

We have considered the parties' arguments and supporting evidence, and we determine that Petitioner has not shown by a preponderance of the evidence that claims 1–8, 12–23, and 27–32 would have been obvious over Yeager and IE5 Resource Kit.

1. *Overview of Yeager and IE5 Resource Kit*

Yeager relates to, *inter alia*, transmitting secure communications over the Web. Ex. 1008, 349. Yeager explains that computers use a Uniform

Resource Locator (“URL”) to locate information on the Web. *Id.* at 5. A URL includes three components: 1) a protocol identifier; 2) a name of a host computer; and 3) a name of a resource. *Id.* at 31; Ex. 1003 ¶ 230. For example, in the URL “http://www.web.org/Stuff/Funny/silly.html,” “http” is the protocol identifier, “www.web.org” is the domain name of the host computer, and “Stuff/Funny/silly.html” is the resource name. Ex. 1008, 31; Ex. 1003 ¶ 230. According to Yeager, one of the leading specifications for secure Web communications is Secure Sockets Layer (“SSL”). Ex. 1008, 349. To enable an SSL secure communication mode, a user must instruct a browser to navigate to a URL that includes the “https” protocol identifier. *Id.*; Ex. 1003 ¶¶ 206, 240. Then, the SSL modules on the client and server establish a secure channel in a manner that is completely transparent to the user. Ex. 1008, 362–363; Ex. 1003 ¶ 208.

IE5 Resource Kit describes various features of the Microsoft Internet Explorer 5 Web browser. Ex. 1006, 1. In particular, IE5 Resource Kit describes an AutoComplete feature that automatically completes a partial URL based on a list of matching sites that a user recently visited. *Id.* at 20. For example, if a user types “http://www.microsoft.com/win” in the browser, the AutoComplete feature may complete the URL to “http://www.microsoft.com/windows.” *Id.* IE5 Resource Kit describes an AutoCorrect feature that automatically corrects an incorrect convention in a URL. *Id.* at 19. For example, if a user types “http;” in the browser, the AutoCorrect feature may change the prefix to “http://.” *Id.* IE5 Resource Kit also describes a feature that automatically adds a domain name suffix to an incomplete URL. *Id.* at 117. For example, if a user types “http://sample”

in the browser, the browser may add the domain name suffix
“.microsoft.com.” *Id.*

2. *Claim 1*

Claim 1 recites “enabling, at the first device, a secure communication mode.” Ex. 1001, col. 55, ll. 49–51. Claim 1 also recites “establishing, based on a determination that the secure communication mode has been enabled, the encrypted communication link between the first device and the second device over the communication network, the establishing including: constructing a domain name based on an identifier associated with the second device.” *Id.* at col. 55, ll. 52–58. Petitioner argues that “[w]hile the claims specify that the step of ‘establishing the encrypted communication link,’ is ‘based on a determination the secure communication mode has been enabled,’ they do not specify that every sub-element of the ‘establishing’ step must be based on that determination.” Pet. Reply 7 (emphasis omitted). Patent Owner, on the other hand, argues that “the steps recited as part of the ‘establishing’ feature of the claims, for instance ‘constructing a domain name,’ occur after the secure communication mode has been enabled.” PO Resp. 36 (emphasis omitted).

We agree with Patent Owner. Claim 1 recites “establishing, based on a determination that the secure communication mode has been enabled, the encrypted communication link.” Ex. 1001, col. 55, ll. 52–54. The phrase “based on” indicates that the encrypted communication link is established *after* a determination is made that the secure communication mode *has been* enabled. *Id.* Claim 1 also specifies that “the establishing include[es]: constructing a domain name.” *Id.* at col. 55, ll. 55–58. In other words, the step of establishing the encrypted communication link (which occurs *after* a

determination is made that the secure communication mode *has been* enabled) includes the step of constructing a domain name. *Id.* Thus, claim 1 requires that the domain name is constructed *after* a determination is made that the secure communication mode *has been* enabled. *Id.* This reading of the claim language is consistent with the specification of the '643 patent, which describes constructing a secure domain name *after* the user enables a secure communication mode by clicking on a “go secure” hyperlink. *Id.* at col. 50, ll. 9–12, col. 50, ll. 20–31.

Petitioner relies on Yeager to teach enabling a secure communication mode. Pet. 24–25, 45–46. Specifically, Petitioner argues that Yeager teaches enabling an SSL secure communication mode in three ways: 1) by clicking on a hyperlink that includes a URL with the “https” protocol identifier; 2) by selecting a button that includes a URL with the “https” protocol identifier; or 3) by typing a URL with the “https” protocol identifier in a browser. *Id.* at 25 (citing Ex. 1008, 349, 353, 361–363).

Petitioner relies on IE5 Resource Kit to teach constructing a domain name. Pet. 46–47. Specifically, Petitioner argues that IE5 Resource Kit teaches an AutoComplete feature that automatically completes a partial URL. Pet. 46 (citing Ex. 1006, 20, 200–201). Petitioner also argues that IE5 Resource Kit teaches an AutoCorrect feature that automatically corrects an incorrect convention in a URL. Pet. 46 (citing Ex. 1006, 19). Lastly, Petitioner argues that IE5 Resource Kit teaches a feature that automatically adds a domain name suffix to an incomplete URL. Pet. 46 (citing Ex. 1006, 114, 117, 267, 427).

Patent Owner contends that combining either of the first two ways for enabling a secure communication mode in Yeager (i.e., clicking on a

hyperlink or selecting a button that includes a URL with the “https” protocol identifier) with the cited features in IE5 Resource Kit would not result in the method recited in claim 1 of the ’643 patent. PO Resp. 33–34. We agree with Patent Owner. As discussed above, claim 1 recites constructing a domain name (Ex. 1001, col. 55, ll. 57–58), and Petitioner argues that IE5 Resource Kit teaches constructing a domain name by completing, adding a suffix to, or correcting a URL (Pet. 46–47). Yeager teaches, though, that when a user clicks on a hyperlink or selects a button to enable an SSL secure communication mode, that hyperlink or button *already* includes a complete and correct URL. Ex. 1008, 356 (“The purchase order form . . . must contain a hypertext link to the security-enhanced form, http://www.vcc.com/scripts/take_orders.html.”), 362 (“The user fills in the form and selects the https hypertext link.”); Ex. 2015 ¶ 56. Because the hyperlink or button in Yeager already includes a complete and correct URL, the cited features in IE5 Resource Kit would not complete, add a suffix to, or correct the URL in the hyperlink or button, and, thus, would not construct a domain name. Ex. 2015 ¶ 56. Petitioner does not dispute this point.¹ See Pet. Reply 5–6. Thus, Petitioner has not shown sufficiently that combining

¹ Petitioner suggests that some adaptation of the cited features in Yeager and IE5 Resource Kit would have been possible, but does not explain specifically what that adaptation would have been. Pet. Reply 6. Petitioner instead just focuses on the third way for enabling a secure communication mode in Yeager. *Id.* at 5–6 (“Patent Owner asserts that Petitioner cannot rely on Yeager’s disclosure of a user clicking on a hyperlink and selecting a button because those actions purportedly are incompatible with the AutoCorrect and AutoComplete features in IE5 Resource Kit. But that argument ignores . . . that another way to navigate to a desired site is by typing the URL into a Web browser.” (emphasis and citations omitted)).

either of the first two ways for enabling a secure communication mode in Yeager with the cited features in IE5 Resource Kit would teach the limitations in claim 1.

Patent Owner also contends that combining the third way for enabling a secure communication mode in Yeager (i.e., typing a URL with the “https” protocol identifier in a browser) with the cited features in IE5 Resource Kit would not result in the method recited in claim 1 of the ’643 patent. PO Resp. 36–38. We agree with Patent Owner. As discussed above, claim 1 requires constructing a domain name *after* a determination is made that a secure communication mode has been enabled. Ex. 1001, col. 55, ll. 52–58. Petitioner does not explain specifically in the Petition how the cited features in IE5 Resource Kit would construct a domain name *after* a determination is made that an SSL secure communication mode has been enabled. See Pet. 24–25, 45–47. The best we can discern from the Petition is that, according to Petitioner, a browser determines that an SSL secure communication mode has been enabled as soon as a user types the “https” portion of a URL, and then the browser completes or corrects the domain name portion of the URL that comes after the “https.” See *id.*

Petitioner, however, does not direct us to specific evidence indicating that a browser determines that an SSL secure communication mode has been enabled as soon as a user types the “https” portion of a URL. See Pet. 24–25, 45–47; Pet. Reply 3–8. In fact, to the contrary, the evidence indicates that a browser only determines that an SSL secure communication mode has been enabled after the browser receives a complete URL and attempts to navigate to that URL. Ex. 1003 ¶ 206 (“This could be accomplished [by] . . . typing the secure protocol *and* address into the web browser.” (emphasis

added)); *id.* ¶ 207 (“[A] user must both activate a secure protocol for Internet Explorer 5 *and* instruct the browser to navigate to a web site using this secure protocol.” (emphasis added)); Ex. 1008, 349 (“[A] URL to be fetched using SSL . . . would be identified as https://www.any.com/example.html.”). To the extent one of the cited features in IE5 Resource Kit constructs a domain name by completing, adding a suffix to, or correcting a URL, those changes are made to the URL *before* the browser attempts to navigate to the URL. Ex. 1006, 19 (“Internet Explorer changes the prefix to http:// and then opens the correct website.”); *id.* at 200 (“AutoComplete . . . completes Web page addresses . . . as the user types them.”); Ex. 2015 ¶ 60. As a result, the domain name is constructed *before* the browser determines that an SSL secure communication mode has been enabled. Ex. 2015 ¶ 60. But, as discussed above, claim 1 requires that the domain name is constructed *after* a determination is made that the secure communication mode has been enabled. Thus, Petitioner has not shown sufficiently that combining the third way for enabling a secure communication mode in Yeager with the cited features in IE5 Resource Kit would teach the limitations in claim 1.

Petitioner argues in the Reply that a browser determines that an SSL secure communication mode has been enabled before a user even starts typing a URL in the browser. Pet. Reply 7. Specifically, Petitioner argues as follows:

As Dr. Tamassia explained, *IE5 would know whether SSL had been enabled*, (Ex. 1003, ¶¶205, 208), and thus, if the user typed in “https” but the browser did not support SSL, AutoCorrect would change the prefix to “http.” See Ex. 1006, 19. If “https” was supported, AutoCorrect would not change it. *Id.* Dr. Monroe agreed. Ex. 1006, 103:1–18.

Pet. Reply 7 (emphasis added). To support this argument, Petitioner cites to a portion of the declaration of Dr. Roberto Tamassia that states “a user must enable one or more secure communication protocols in the Internet Explorer 5 browser, such as SSL 2.0, SSL 3.0, TLS 1.0, or PCT 1.0, *by checking the appropriate boxes in the Internet Options configuration window.*” Ex. 1003 ¶ 205 (emphasis added).

As an initial matter, Petitioner’s argument in the Reply is improper. “A reply may only respond to arguments raised in the . . . patent owner response.” 37 C.F.R. § 42.23(b). As discussed above, Petitioner argues in the Petition that an SSL secure communication mode can be enabled in three ways: 1) by clicking on a hyperlink that includes a URL with the “https” protocol identifier; 2) by selecting a button that includes a URL with the “https” protocol identifier; or 3) by typing a URL with the “https” protocol identifier in a browser. Pet. 25 (citing Ex. 1008, 349, 353, 361–363). Petitioner does not argue specifically in the Petition that an SSL secure communication mode can be enabled by checking an SSL box in a configuration window in Internet Explorer, or that a browser determines that an SSL secure communication mode has been enabled before a user even starts typing a URL. See Pet. 24–25. Thus, because Petitioner presents this theory of unpatentability for the first time in the Reply, it is improper. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369–70 (Fed. Cir. 2016); *Ariosa Diagnostics v. Verinata Health, Inc.*, 805 F.3d 1359, 1367–68 (Fed. Cir. 2015).

Moreover, even if Petitioner’s argument in the Reply is proper, it is not persuasive for several reasons. First, the evidence does not support Petitioner’s argument that a browser determines that an SSL secure

communication mode has been enabled before a user even starts typing a URL. Petitioner's declarant, Dr. Tamassia, acknowledges "that to use SSL encryption in the Internet Explorer web browser, a user must *both* activate a secure protocol for Internet Explorer 5 *and* instruct the browser to navigate to a web site using this secure protocol." Ex. 1003 ¶ 207 (emphasis added). In other words, a browser does not determine that an SSL secure communication mode has been enabled just because a user checks an SSL box in a configuration window. *Id.* Rather, a browser determines that an SSL secure communication mode has been enabled when a user checks the SSL box *and*, as discussed above, instructs the browser to navigate to a URL with the "https" protocol identifier. *Id.* ¶¶ 206, 207

Second, the evidence does not support Petitioner's argument that the AutoCorrect feature described in IE5 Resource Kit would change the protocol identifier from "https" to "http" based on the SSL configuration settings in the browser.² The portion of IE5 Resource Kit cited by Petitioner teaches that the AutoCorrect feature may change an incorrect URL convention, such as by changing "http" to "http." Ex. 1006, 19. Importantly, though, "https" and "http" both are correct URL conventions. Ex. 1003 ¶¶ 206, 235, 240. The portion of IE5 Resource Kit cited by Petitioner does not teach or suggest that the AutoCorrect feature will check

² Petitioner argues that Patent Owner's declarant, Dr. Fabian Monroe, agrees with Petitioner's position. Pet. Reply 7. However, in the deposition testimony cited by Petitioner, Dr. Monroe only states that Internet Explorer recognizes the "https" protocol, *not* that the AutoCorrect feature would change the protocol identifier from "https" to "http" based on the SSL configuration settings in the browser. Ex. 1046, 103:1–18.

the SSL configuration settings in the browser and then change an otherwise correct URL convention based on those settings. See Ex. 1006, 19.

Third, even if the AutoCorrect feature would change the protocol identifier from “https” to “http,” it still does not teach the limitations in claim 1. As discussed above, claim 1 recites constructing a *domain name*. Ex. 1001, col. 55, ll. 57–58. Petitioner’s declarant, Dr. Tamassia, acknowledges that a domain name is different than a protocol identifier. Ex. 1003 ¶ 230. Thus, just changing the protocol identifier from “https” to “http” does not teach constructing a domain name. Claim 1 also recites that the step of constructing a domain name is part of the step of establishing an *encrypted* communication link. Ex. 1001, col. 55, ll. 52–58. However, if the AutoCorrect feature changes the protocol identifier from “https” to “http,” then the browser will establish a regular communication link, not an encrypted communication link. Ex. 1003 ¶¶ 206, 235, 240.

For the foregoing reasons, we determine that Petitioner has not shown by a preponderance of the evidence that claim 1 would have been obvious over Yeager and IE5 Resource Kit.

3. Claim 17

Claim 17 recites limitations similar to those discussed above with respect to claim 1. Specifically, claim 17 recites “at least one processor that executes the instructions to: enable a secure communication mode . . . and establish, based on a determination that the secure communication mode has been enabled, the encrypted communication link . . . the establishing including: constructing a domain name based on an identified associated with the second device.” Ex. 1001, col. 57, ll. 18–28. Petitioner relies on

the same arguments and evidence that it presented for claim 1.³ Pet. 23–30, 45–47. Therefore, for the same reasons discussed above with respect to claim 1, we determine that Petitioner has not shown by a preponderance of the evidence that claim 17 would have been obvious over Yeager and IE5 Resource Kit. *See supra* Section II.B.2.

4. *Claims 2–8, 12–16, 18–23, and 27–32*

Claims 2–8, 12–16, 18–23, and 27–32 depend, directly or indirectly, from claim 1 or claim 17. Therefore, for the same reasons discussed above with respect to claims 1 and 17, we determine that Petitioner has not shown by a preponderance of the evidence that claims 2–8, 12–16, 18–23, and 27–32 would have been obvious over Yeager and IE5 Resource Kit. *See supra* Sections II.B.2–II.B.3.

C. *Obviousness of Claims 9 and 24 Over Yeager, IE5 Resource Kit, and RFC 1034*

Petitioner argues that claims 9 and 24 would have been obvious over Yeager, IE5 Resource Kit, and RFC 1034. Pet. 3. Claim 9 depends indirectly from claim 1, and claim 24 depends indirectly from claim 17. Petitioner does not argue that RFC 1034 compensates for any of the deficiencies discussed above with respect to claims 1 and 17. *See* Pet. 50. Therefore, for the same reasons discussed above with respect to claims 1 and 17, we determine that Petitioner has not shown by a preponderance of the evidence that claims 9 and 24 would have been obvious over Yeager, IE5 Resource Kit, and RFC 1034. *See supra* Sections II.B.2–II.B.3.

³ Neither party argues that claim 17 should be treated differently than claim 1 because it is a system claim.

D. *Patent Owner's Motion to Exclude*

Patent Owner filed a Motion to Exclude (Paper 27, "PO Mot. Excl."), to which Petitioner filed an Opposition (Paper 29, "Pet. Opp. Excl."), and Patent Owner filed a Reply (Paper 30, "PO Reply Excl."). Patent Owner argues that Exhibits 1002, 1004, 1007, 1009, 1014, 1017, 1018, 1021–1023, 1025–1036, 1042, and 1048–1053, and portions of Exhibit 1003 should be excluded. PO Mot. Excl. 1. We have considered the parties' arguments, and, for the reasons discussed below, Patent Owner's Motion to Exclude is *denied in part and dismissed in part*.

1. *Exhibits 1002, 1004, 1007, 1009, 1014, 1017, 1018, 1021–1023, 1025–1036, and 1042*

Patent Owner argues that Exhibits 1002, 1004, 1007, 1009, 1014, 1017, 1018, 1021–1023, 1025–1036, and 1042 should be excluded under Fed. R. Evid. 401, 402, and 403, because Petitioner does not cite to those exhibits in the Petition or the Reply, and, thus, has not established the relevance of those exhibits. PO Mot. Excl. 5–6. Patent Owner's argument is not persuasive. To the extent Petitioner fails to explain sufficiently the relevance of evidence in the Petition or the Reply, we may decide to give that evidence no weight, rather than exclude it. 37 C.F.R. § 42.104(b)(5). Therefore, Patent Owner's Motion to Exclude Exhibits 1002, 1004, 1007, 1009, 1014, 1017, 1018, 1021–1023, 1025–1036, and 1042 is *denied*.

2. *Exhibit 1003*

Patent Owner argues that those portions of Exhibit 1003 that are not cited in the Petition or the Reply should be excluded under Fed. R. Evid. 401, 402, and 403, because Petitioner has not established the relevance of those portions of Exhibit 1003. PO Mot. Excl. 6. Patent Owner's argument is not persuasive. To the extent Petitioner fails to explain sufficiently the

relevance of evidence in the Petition or the Reply, we may decide to give that evidence no weight, rather than exclude it. 37 C.F.R. § 42.104(b)(5). Therefore, Patent Owner's Motion to Exclude certain portions of Exhibit 1003 is *denied*.

3. *Exhibits 1048–1053*

Patent Owner argues that Exhibits 1048–1053 should be excluded under Fed. R. Evid. 801 and 802, as inadmissible hearsay. PO Mot. Excl. 2. Petitioner relies on Exhibits 1048–1053 to show that RFC 1034 is a prior art printed publication. Pet. Reply 17–19; PO Mot. Excl. 2. Petitioner only includes RFC 1034 in the asserted ground of unpatentability for claims 9 and 24. Pet. 3. For the reasons discussed above, we determine that Petitioner has not shown by a preponderance of the evidence that claims 9 and 24 would have been obvious over Yeager, IE5 Resource Kit, and RFC 1034. *See supra* Section II.C. As a result, we do not reach the parties' arguments regarding whether RFC 1034 is a prior art printed publication, and we do not rely on Exhibits 1048–1053 in this Decision. Therefore, Patent Owner's Motion to Exclude Exhibits 1048–1053 is *dismissed* as moot.

III. CONCLUSION

Petitioner has not shown by a preponderance of the evidence that claims 1–9, 12–24, and 27–32 of the '643 patent are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–9, 12–24, and 27–32 of the '643 patent are not shown unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is *denied in part and dismissed in part*; and

IPR2015-01010
Patent 8,843,643 B2

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

IPR2015-01010
Patent 8,843,643 B2

PETITIONER:

Jeffrey P. Kushan
Scott Border
Thomas A. Broughan III
SIDLEY AUSTIN LLP
IPRNotices@sidley.com
sborder@sidley.com
tbroughan@sidley.com

PATENT OWNER:

Joseph E. Palys
Naveen Modi
Daniel Zeilberger
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com
danielzeilberger@paulhastings.com