

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-01009
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)
1–9, 12, 14, 17–24, 27, and 29	35 U.S.C. § 102(a)	Microsoft Windows 2000 Professional Resource Kit (2000) (Ex. 1005, “Windows Resource Kit”)
1, 13, 15–17, 28, and 30–32	35 U.S.C. § 103(a)	Windows Resource Kit; Microsoft Internet Explorer 5 Resource Kit (1999) (Ex. 1006, “IE5 Resource Kit”); and Elgamal et al., U.S. Patent No. 5,657,390 (issued Aug. 12, 1997) (Ex. 1007, “Elgamal”)

Paper 9 (“Dec. on Inst.”), 9.

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 shown by a preponderance of the evidence that claims 1–9, 14, 17–24, and 29 of the ’643 patent are unpatentable, but Petitioner has not shown by a preponderance of the evidence that claims 12, 13, 15, 16, 27, 28, and 30–32 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 IPR2015-01010, 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. 8–14; PO Resp. 4–22. 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. *Anticipation of Claims 1–9, 12, 14, 17–24, 27, and 29 by Windows Resource Kit*

Petitioner argues that claims 1–9, 12, 14, 17–24, 27, and 29 are anticipated by Windows Resource Kit. Pet. 3. A claim is anticipated if each limitation of the claim is disclosed in a single prior art reference arranged as in the claim. *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). We have considered the parties’ arguments and supporting evidence. We determine that Petitioner has shown by a preponderance of the evidence that claims 1–9, 14, 17–24, and 29 are anticipated by Windows Resource Kit, but Petitioner has not shown by a preponderance of the evidence that claims 12 and 27 are anticipated by Windows Resource Kit.

1. *Overview of Windows Resource Kit*

Windows Resource Kit is a guide for installing, configuring, and supporting Windows 2000. Ex. 1005, xxxiii. Windows Resource Kit describes, *inter alia*, configuring a computer with Windows 2000 to communicate with other computers on a network. *Id.* at 948. For example, Windows Resource Kit explains that a user can select a security policy on a Windows 2000 computer to ensure that communications with other computers are secure. *Id.* at 1021–1025. Windows Resource Kit also describes the Domain Name System (“DNS”) that a Windows 2000 computer uses to communicate with other computers on a network. *Id.* at 964. Specifically, Windows Resource Kit explains that a Windows 2000 computer sends a query containing a domain name associated with another

computer to a DNS. *Id.* The DNS then responds to the query with an Internet Protocol (“IP”) address. *Id.* at 964, 986. The Windows 2000 computer uses that IP address to locate the other computer on the network. *Id.* at 1006. Based on the security policy selected on the Windows 2000 computer, the two computers may establish an encrypted communication link. *Id.* at 1021–1022.

2. *Claim 1*

Claim 1 recites “enabling, at the first device, a secure communication mode without a user entering any cryptographic information for establishing the secure communication mode.” Ex. 1001, col. 55, ll. 49–51. Windows Resource Kit discloses enabling a secure communication mode on a computer by selecting one of several default IP security policies using an IP security dialog box and without entering any other information. Pet. 20–21; Ex. 1003 ¶¶ 188–189; Ex. 1005, 1024–1025. The “Secure Server” (or “High”) policy, for example, requires that “all outgoing communications are secured” and that “[a]ll unsecured incoming communications are rejected.” Pet. 21; Ex. 1003 ¶¶ 189–190; Ex. 1005, 1025.

Patent Owner argues that Windows Resource Kit does not disclose enabling a secure communication mode *without* a user entering any cryptographic information. PO Resp. 22–24. Specifically, Patent Owner argues that Windows Resource Kit requires the user to select a security policy, and, thus, requires the user to identify a specific encryption function. *Id.* at 23–24 (citing Ex. 2015 ¶¶ 38–39). Patent Owner’s argument is not persuasive. Neither Patent Owner nor Patent Owner’s declarant, Dr. Fabian Monroe, explains specifically how selecting one of the default IP security policies in Windows Resource Kit identifies a specific encryption function.

PO Resp. 22–24; Ex. 2015 ¶¶ 38–39; Ex. 1046, 74:14–75:22. Further, contrary to Patent Owner’s argument, Windows Resource Kit discloses that selecting one of the default IP security policies simply indicates *whether* a communication is secure, not a specific encryption function. Ex. 1003 ¶¶ 189–190; Ex. 1005, 1024–1025. This disclosure in Windows Resource Kit is consistent with the written description in the ’643 patent, which explains that clicking a “go secure” hyperlink indicates *whether* a communication is secure, but not a specific encryption function. Ex. 1001, col. 50, ll. 9–19.

Claim 1 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.” Ex. 1001, col. 55, ll. 52–55. Windows Resource Kit discloses the procedure for establishing an IP security session between a first computer (Computer A) and a second computer (Computer B). Pet. 22–23; Ex. 1003 ¶¶ 195–198; Ex. 1005, 1021–1022, Fig. 22.19. Specifically, Windows Resource Kit states the following:

2. IPsec checks IP Security Group Policy settings on Computer A to determine the computer’s active IP Security policy. The default policies allow a computer to demand secure communication, to request secure communication but proceed unsecurely if necessary, or to never request IP security.
3. Computer A begins security negotiations with Computer B. The two computers exchange public keys and establish a shared, secret key that is created independently at both ends without being transmitted across the network.

Ex. 1005, 1021–1022. In other words, Windows Resource Kit discloses that the first computer determines which IP security policy was selected by the

user, and, based on that determination, begins negotiations with the second computer to establish an encrypted communication link. Ex. 1003 ¶¶ 185–186, 197–198; Ex. 1005, 1021–1022, Fig. 22.19.

Patent Owner argues that Windows Resource Kit does not disclose establishing an encrypted communication link *based on* a determination that the secure communication mode has been enabled because selecting an IP security policy in Windows Resource Kit does not *trigger* the establishment of an encrypted communication link between two computers. PO Resp. 25–28 (citing Ex. 2015 ¶¶ 42–46). Patent Owner’s argument is not persuasive. Claim 1 recites that establishing the encrypted communication link is “based on” a determination that the secure communication mode has been enabled. Ex. 1001, col. 55, ll. 52–55. In contrast, claim 16, which depends from claim 1, recites that establishing the encrypted communication link is “trigger[ed]” by enablement of the secure communication mode. *Id.* at col. 57, ll. 9–11. The use of different terms in claims 1 and 16 indicates that the phrase “based on” in claim 1 is not limited to the “trigger[ing]” recited in claim 16. *See Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004).

The specification of the ’643 patent also indicates that the phrase “based on” in claim 1 does not require triggering the establishment of an encrypted communication link. Although, as Patent Owner points out, the ’643 patent describes an embodiment in which clicking a “go secure” hyperlink triggers the establishment of an encrypted communication link (PO Resp. 27–28 (citing Ex. 1001, col. 49, ll. 44–46, col. 50, ll. 9–22, Fig. 34)), the ’643 patent is not limited to that embodiment. For example, the ’643 patent also explains that “the user can optionally specify that all

communication links established over computer network 3302 are secure communication links” and, thus, “anytime that a communication link is established, the link is a VPN link.” Ex. 1001, col. 52, ll. 10–14. In other words, a user can enable a secure communication mode once for all future communication links so that “the user need not ‘click’ on the secure option each time secure communication is to be effected.” *Id.* at col. 52, ll. 16–19. As such, in this embodiment in the ’643 patent, the establishment of an encrypted communication link is based on, but not triggered by, a determination that the secure communication mode has been enabled.

Claim 1 recites that establishing the encrypted communication link includes “constructing a domain name based on an identifier associated with the second device.” Ex. 1001, col. 55, ll. 55–58. Windows Resource Kit discloses constructing a domain name by appending a DNS suffix to a DNS host name. Pet. 24–27; Ex. 1003 ¶¶ 162–163; Ex. 1005, 967–968, 972, 976. For example, Windows Resource Kit discloses that the DNS suffix “dom1.acquired01-int.com” is appended to the DNS host name “client1” to construct the domain name “client1.dom1.acquired01-int.com.” Pet. 25; Ex. 1003 ¶ 165; Ex. 1005, 976. The DNS host name “client1” is a name used to identify the second computer. Ex. 1003 ¶ 165; Ex. 1005, 968 (“The DNS host name is taken from the computer name assigned to it during Windows 2000 Professional installation.”). Patent Owner does not dispute that Windows Resource Kit discloses the above limitation of claim 1.

Claim 1 recites that establishing the encrypted communication link includes “sending a query using the domain name.” Ex. 1001, col. 55, l. 59. Windows Resource Kit discloses that the first computer sends a query containing the domain name to a DNS. Pet. 27; Ex. 1003 ¶¶ 161, 165; Ex.

1005, 964, 976. Patent Owner does not dispute that Windows Resource Kit discloses the above limitation of claim 1.

Claim 1 recites that establishing the encrypted communication link includes “receiving, in response to the query, at least one network address associated with the domain name.” Ex. 1001, col. 55, ll. 60–61. Windows Resource Kit discloses that, in response to the query, the first computer receives one or more IP addresses associated with the domain name from the DNS. Pet. 28; Ex. 1003 ¶¶ 172, 174–175; Ex. 1005, 964 (“When a request for name-to-IP address resolution is made, the Windows 2000 resolver first submits the name query to DNS.”), 986. Patent Owner does not dispute that Windows Resource Kit discloses the above limitation of claim 1.

Claim 1 recites that establishing the encrypted communication link includes “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. 62–67. Windows Resource Kit discloses that to establish the encrypted communication link, the first computer sends a packet to the second computer that includes the IP address received from the DNS. Pet. 29; Ex. 1003 ¶¶ 195–196; Ex. 1005, 964, 1006 (“When IP prepares to send a packet, it inserts the local (source) IP address and the destination address.”), 1021. Windows Resource Kit also discloses that to establish the encrypted communication link, the first computer uses a public encryption key received from the second computer. Pet. 29–30; Ex. 1003 ¶¶ 198, 202; Ex. 1005, 1022 (“The two computers exchange public keys and establish a shared, secret key.”). Windows Resource Kit discloses

that the second computer can be a server. Ex. 1005, 1025 (“Secure Server (Require Security)”).

Patent Owner argues that the first computer in Windows Resource Kit “could come pre-configured with the IP address” of the second computer, and, thus, the IP address would not be received from a server separate from the first computer. PO Resp. 29–30 (citing Ex. 2015 ¶¶ 48–49). Patent Owner’s argument is not persuasive. Patent Owner does not direct us to any specific portion of Windows Resource Kit that discloses a computer coming pre-configured with the IP address of another computer. PO Resp. 29–30. Further, as discussed above, Windows Resource Kit expressly discloses that the first computer receives the IP address of the second computer from a DNS that is separate from the first computer. Ex. 1003 ¶¶ 172, 174–175; Ex. 1005, 964 (“When a request for name-to-IP address resolution is made, the Windows 2000 resolver first submits the name query to DNS.”), 986.

Patent Owner also argues that Petitioner improperly relies on the second computer in Windows Resource Kit as teaching both the server and the second device in claim 1. PO Resp. 30–32 (citing Ex. 2015 ¶¶ 50–52). Patent Owner contends that, according to the specification of the ’643 patent, the server that provides the encrypted communication link resources must be separate from the first device *and* the second device. PO Resp. 31 (citing Ex. 1001, col. 51, ll. 29–42, col. 51, ll. 57–62, Fig. 33).

Patent Owner’s argument is not persuasive. Claim 1 recites a “first device,” a “second device,” and a “server” separately, which generally is an indication that those elements are distinct components. Ex. 1001, col. 55, ll. 62–67; *see Becton, Dickinson & Co. v. Tyco Healthcare Group, LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (“Where a claim lists elements separately,

‘the clear implication of the claim language’ is that those elements are ‘distinct component[s]’ of the patented invention.”). However, the parties agree that the term “server,” when given its ordinary and customary meaning, can refer to software operative on a computer. Pet. Reply 11; Tr. 33:11–15. In other words, although the term “server” is recited separately in claim 1, the ordinary and customary meaning of the term “server” indicates that it can be part of a computer. *Id.* Further, claim 1 specifies that the server is “separate from” the first device, but does not recite a similar requirement that the server is separate from the second device. Ex. 1001, col. 55, ll. 62–67. Thus, the claim language indicates that the server is separate from the first device, but not necessarily the second device. *Id.*; see *Retractable Techs., Inc. v. Becton, Dickson & Co.*, 653 F. 3d 1296, 1303 (Fed. Cir. 2011) (holding that the claim language indicates that the “needle holder” and “retainer member” need not be separate components).

Our reading of the claim language is consistent with the specification of the ’643 patent. One embodiment described in the ’643 patent includes computer 2601 (a first device), computer with unsecure target site 2611 and secure target site 2604 (a second device), and gatekeeper 2603 (a server) that provides encrypted communication link resources. Ex. 1001, col. 39, ll. 58–67, col. 40, ll. 10–14, Fig. 26. Another embodiment described in the ’643 patent includes computer 3301 (a first device), computer with unsecure server 3304 and secure server 3320 (a second device), and gatekeeper 3314 (a server) that provides encrypted communication link resources. *Id.* at col. 49, ll. 10–13, col. 51, ll. 29–39, Fig. 33. In each of those embodiments, the server is separate from both the first and second devices. *Id.* at Figs. 26, 33.

There is, however, another embodiment in the '643 patent that includes computer 3604 (a first device), computer 3608 (a second device), and server proxy 3610 (a server) that provides encrypted communication link resources.¹ *Id.* at col. 53, ll. 57–58, col. 54, ll. 40–43, col. 55, ll. 9–21, Fig. 36. In this embodiment, server proxy 3610, which provides encrypted communication link resources to computer 3604, is separate from computer 3604 (the first device), but is part of computer 3608 (the second device). *Id.* at col. 55, ll. 9–23, Fig. 36. Thus, like the claim language, this embodiment in the specification indicates that the server is separate from the first device, but not necessarily the second device. *Id.*; see *Powell v. Home Depot U.S.A., Inc.*, 663 F.3d 1221, 1231–32 (Fed. Cir. 2011) (holding that the specification discloses that the “cutting box” may also function as a “dust collection structure,” and, thus, the claim terms do not require separate components).

At the oral hearing, Patent Owner argued that the '643 patent indicates that the first device accesses the server *before* the encrypted communication link is established, but does not access the second device until *after* the encrypted communication link is established. Tr. 30:17–31:5 (citing Ex. 1001, col. 51, ll. 31–32). Thus, according to Patent Owner, the server cannot be part of the second device. Tr. 30:17–31:5. Patent Owner's argument is not persuasive. The '643 patent indicates that the second device

¹ The embodiment in Figure 36 differs from those in Figures 26 and 33 because it creates a virtual private connection, rather than a VPN. Ex. 1001, col. 53, l. 66–col. 54, l. 8. Nonetheless, like the gatekeepers in Figures 26 and 33, the server proxy in Figure 36 provides field-hopping resources, such as those used for a VPN. *Id.* at col. 40, ll. 32–35, col. 51, ll. 57–64, col. 55, ll. 14–17.

in Figure 33 may include unsecure server 3304 *and* secure server 3320. Ex. 1001, col. 51, ll. 29–39, Fig. 33. Although the first device can only access secure server 3320 after the encrypted communication link is established (*id.* at col. 51, ll. 31–32), the first device can access unsecure server 3304 and any other unsecure portions of the second device before the encrypted communication link is established (*id.* at col. 49, ll. 28–30). Thus, contrary to Patent Owner’s argument, the first device can access the unsecure portions of the second device to obtain the encrypted communication link resources and then use those resources to establish an encrypted communication link with the secure server on the second device. *See, e.g., id.* at col. 55, ll. 9–23, Fig. 36.

For the reasons discussed above, we determine that Petitioner has shown by a preponderance of the evidence that claim 1 is anticipated by Windows Resource Kit.

3. *Claim 17*

Claim 17 recites limitations similar to those discussed above with respect to claim 1. Ex. 1001, col. 57, ll. 12–37; *see supra* Section II.B.2. Claim 17 further specifies that the first device comprises “a communications component that communicates over the communication network,” “a memory storing computer program instructions,” and “at least one processor that executes the instructions.” Ex. 1001, col. 57, ll. 15–18. Windows Resource Kit discloses a computer with a network adapter for communicating over a communication network (Pet. 31; Ex. 1003 ¶ 157; Ex. 1005, 84 (“detects your network adapter”), 107), a memory for storing computer program instructions (Pet. 31; Ex. 1003 ¶ 157; Ex. 1005, 107), and a processor for executing those instructions (Pet. 31; Ex. 1003 ¶ 157; Ex.

1005, 107). Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claim 17.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claim 17 is anticipated by Windows Resource Kit.

4. *Claims 2, 4, and 18*

Claim 2 depends from claim 1, and recites “wherein enabling the secure communication mode includes receiving a command entered into the first device by the user, and the command specifies the secure communication mode.” Ex. 1001, col. 56, ll. 1–4. Windows Resource Kit discloses that a user can enable a secure communication mode on a computer by selecting one of several default IP security policies using an IP security dialog box on the computer. Pet. 32–33; Ex. 1003 ¶¶ 188–189; Ex. 1005, 1024–1025. Selecting the “Secure Server” (or “High”) policy, for example, specifies a secure communication mode because it requires that “all outgoing communications are secured” and that “[a]ll unsecured incoming communications are rejected.” Pet. 32–33; Ex. 1003 ¶¶ 189–190; Ex. 1005, 1025. Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claim 2.

Claim 4 depends from claim 2, and recites “wherein receiving the command includes: displaying, at the first device, a user interface including a user interface element for enabling the secure communication mode; and receiving the command from the user via the user interface element.” Ex. 1001, col. 56, ll. 8–14. Windows Resource Kit discloses a computer that displays Windows 2000, which is a user interface (Pet. 33; Ex. 1005, 7 (“Windows 2000 Professional has an improved user interface.”)), and displays an IP security dialog box, which is a user interface element (Pet. 33;

Ex. 1005, 1025). Windows Resource Kit discloses that a user can enable a secure communication mode on the computer by selecting one of several default IP security policies using the IP security dialog box. Pet. 33–34; Ex. 1003 ¶¶ 188–189; Ex. 1005, 1024–1025. Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claim 4.

Claim 18 depends from claim 17, and recites limitations similar to those discussed above with respect to claims 2 and 4. Ex. 1001, col. 57, ll. 38–48. For the reasons discussed above with respect to claims 2 and 4, Windows Resource Kit discloses the limitations of claim 18. Patent Owner does not dispute that Windows Resource Kit discloses the limitations of claim 18.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 2, 4, and 18 are anticipated by Windows Resource Kit.

5. *Claims 3 and 19*

Claim 3 depends from claim 2, and recites “wherein the command defines a setup parameter associated with the secure communication mode.” Ex. 1001, col. 56, ll. 5–7. Claim 19 depends from claim 17, and recites similar limitations. *Id.* at col. 57, ll. 49–51. As discussed above, Windows Resource Kit discloses that a user can enable a secure communication mode on a computer by selecting one of several default IP security policies using an IP security dialog box. Pet. 36; Ex. 1003 ¶¶ 188–189; Ex. 1005, 1024–1025. The default IP security policies are setup parameters because they determine which communications are secure. Pet. 36; Ex. 1003 ¶¶ 189–190; Ex. 1005, 1024–1025. Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claims 3 and 19.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 3 and 19 are anticipated by Windows Resource Kit.

6. *Claims 5 and 20*

Claim 5 depends from claim 4, and recites “wherein the user interface comprises an application stored on the first device.” Ex. 1001, col. 56, ll. 16–17. Claim 20 depends from claim 17, and recites similar limitations. *Id.* at col. 57, ll. 52–53. As discussed above, Windows Resource Kit discloses a computer that displays Windows 2000, which is a user interface. Pet. 37; Ex. 1005, 7. Windows Resource Kit further discloses that Windows 2000 includes an Internet Explorer 5 application that is stored on the computer. Pet. 37; Ex. 1005, 11–12 (“With Internet Explorer 5 built in”). Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claims 5 and 20.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 5 and 20 are anticipated by Windows Resource Kit.

7. *Claims 6 and 21*

Claim 6 depends from claim 5, and recites “wherein the application comprises a web browser.” Ex. 1001, col. 56, ll. 18–19. Claim 21 depends from claim 20, and recites similar limitations. *Id.* at col. 57, ll. 54–55. As discussed above with respect to claims 4 and 5, Windows Resource Kit discloses a computer with Windows 2000, which is a user interface. Pet. 37; Ex. 1005, 7. Windows Resource Kit further discloses that Windows 2000 includes an Internet Explorer 5 application, which is a web browser. Pet. 37; Ex. 1005, 11–12.

Patent Owner argues that, because claim 6 depends indirectly from claim 4, claim 6 requires that the user interface recited in claim 4 comprise a web browser. PO Resp. 32–33 (citing Ex. 2015 ¶¶ 53–54). Patent Owner contends that Petitioner relies on the IP security dialog box in Windows Resource Kit as disclosing the user interface in claim 4, but does not show that the IP security dialog box includes a web browser. PO Resp. 33–34 (citing Ex. 2015 ¶¶ 55–57).

Patent Owner’s argument is not persuasive. Petitioner relies on Windows 2000, not the IP security dialog box, in Windows Resource Kit as disclosing the “user interface” recited in claims 4 and 18. Pet. 33 (“Windows Resource Kit further discloses that the user interface in Windows 2000 provides multiple user interface elements, including the IP security dialog window.” (emphasis omitted)). Petitioner relies on the IP security dialog box as disclosing the “user interface element” recited in claims 4 and 18. *Id.* Claims 6 and 21 recite that the *user interface* comprises a web browser application. Ex. 1001, col. 56, ll. 16–19, col. 57, ll. 52–55. Thus, Petitioner must show that Windows 2000 (i.e., the user interface) comprises a web browser application, but does not have to show that the IP security dialog box (i.e., the user interface element) comprises a web browser application. *Id.* As discussed above, Windows Resource Kit discloses that Windows 2000 includes an Internet Explorer 5 application, which is a web browser. Pet. 37; Ex. 1005, 11–12.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 6 and 21 are anticipated by Windows Resource Kit.

8. *Claims 7 and 22*

Claim 7 depends from claim 1, and recites “wherein sending the query using the domain name includes sending, to a secure domain name service (SDNS), a query for a network address associated with the domain name.” Ex. 1001, col. 56, ll. 20–23. Claim 22 depends from claim 17, and recites similar limitations. *Id.* at col. 57, ll. 56–59.

Petitioner argues that a secure domain name service (“SDNS”) is “a service that provides a secure computer network address for a requested secure domain name.” Pet. 12. Petitioner further specifies that a secure domain name is “a name that corresponds to a secure computer network address.” *Id.* (emphasis omitted). Patent Owner argues that an SDNS is “a lookup service that recognizes that a query message is requesting a secure computer network address, i.e., a network address that requires authorization for access, and returns a secure computer network address for a requested secure domain name.” PO Resp. 13. Patent Owner further specifies that a secure domain name is “a non-standard domain name that corresponds to a secure computer network address, i.e., a network address that requires authorization for access, and cannot be resolved by a conventional domain name service (DNS).” *Id.* at 5. For the reasons discussed below, we determine that Petitioner has shown sufficiently that Windows Resource Kit discloses the limitations of claims 7 and 22 under either proposed construction. Thus, we need not adopt either proposed construction to resolve the parties’ dispute regarding claims 7 and 22.

Windows Resource Kit discloses sending a query using a domain name to a DNS. Pet. 27, 38; Ex. 1003 ¶¶ 161, 165; Ex. 1005, 964, 976. Windows Resource Kit discloses a DNS that is located on a corporate

intranet and returns IP addresses for computers connected to the corporate intranet. Pet. 39; Ex. 1005, 989–990, Fig. 22.12. Windows Resource Kit also discloses that the computers connected to the corporate intranet can be configured to have a “Secure Server” (or “High”) policy so that those computers require authorization for access and secure communications. Pet. 21, 38; Pet. Reply 13; Ex. 1003 ¶¶ 183, 189–190; Ex. 1005, 1020 (“Authentication methods limit access from unauthorized users.”), 1024 (“IPSec policies can be selected” on a “computer . . . [that] is connected to other hosts by means of an enterprise *intranet*.” (emphasis added)), 1025 (“Requires that all communications . . . be secured.”). Thus, Windows Resource Kit discloses a DNS on a corporate intranet that resolves domain names into IP addresses for computers that require authorization for access and secure communications.² Ex. 1003 ¶¶ 183, 189–190; Ex. 1005, 989–990, 1020, 1024–1025, Fig. 22.12.

Windows Resource Kit further discloses that a computer connected to both the corporate intranet and the Internet can be assigned a different domain name and different IP address for each connection. Pet. 39; Ex. 1005, 971 (“For each connection, you can specify a connection-specific domain name.”), 990 (“[I]f you have a client that is connected to two different networks, and you want it to have a different domain name on each network, you can configure it to do so.”). For example, the connection to the corporate intranet can be assigned the domain name

² We note that this is consistent with the evidence Patent Owner presented in *VirnetX, Inc. v. Cisco Systems, Inc.*, 767 F.3d 1308, 1321–22 (Fed. Cir. 2014), which indicates that communications between computers on a private corporate intranet are secure.

“Client1.reskit.com,” and the connection to the Internet can be assigned the domain name “Client1.isp01-ext.com.” *Id.* at 971, Fig. 22.4. The corporate intranet domain name corresponds to a specific IP address and is registered only with the corporate intranet DNS “NoamDC1.” *Id.* at 989–990, Fig. 22.12. On the other hand, the Internet domain name corresponds to a different IP address and is registered only with a public DNS “ISPNameServer.” *Id.* Thus, the corporate intranet DNS in Windows Resource Kit resolves domain names that cannot be resolved by the public DNS. *Id.* at 971, 989–990, Figs. 22.4, 22.12.

Patent Owner argues that Windows Resource Kit does not disclose secure computers because “depending on the selected policy, ‘[c]ommunications are unsecured if the requesting host is not IPsec-enabled.’” PO Resp. 36 (citing Ex. 1005, 1021, 1025). Patent Owner’s argument is not persuasive. As discussed above, Windows Resource Kit discloses a “Secure Server” (or “High”) policy, which requires that “all outgoing communications are secured” and “[a]ll unsecured incoming communications are rejected.” Ex. 1005, 1025. In other words, when the “High” security policy is selected on a computer, *all* communications with that computer are secure, regardless of the security policy selected on other computers. *Id.*

Patent Owner argues that the domain names disclosed in Windows Resource Kit are not non-standard domain names. PO Resp. 37 (citing Ex. 2015 ¶ 63). Patent Owner’s argument is not persuasive. Patent Owner does not explain specifically what it means for a domain name to be non-standard or why the domain names in Windows Resource Kit are not non-standard. PO Resp. 37; Tr. 47:8–49:16; Ex. 2015 ¶ 63. Moreover, the ’643 patent

indicates that a non-standard domain name involves a top-level domain name that cannot be resolved by a conventional public DNS. Ex. 1001, col. 50, ll. 19–35. As discussed above, Windows Resource Kit discloses domain names that are registered only with a corporate intranet DNS, and, thus, can be resolved only by the corporate intranet DNS. Ex. 1005, 971, 989 (“Client1 resolves intranet names by using a name server on the intranet, NoamDC1, and resolves Internet names by using a name server on the Internet, ISPNameServer.”), 990, Figs. 22.4, 22.12. Those domain names are non-standard domain names because, like the non-standard domain names described in the ’643 patent, they cannot be resolved by a conventional public DNS. Ex. 1001, col. 50, ll. 32–35; Ex. 1005, 971, 989–990, Figs. 22.4, 22.12.

Patent Owner argues that Windows Resource Kit does not disclose a DNS that returns an address requiring authorization for access. PO Resp. 37 (citing Ex. 2015 ¶ 63). Patent Owner’s argument is not persuasive. As discussed above, Windows Resource Kit discloses that computers connected to a corporate intranet can be configured to have a “Secure Server” (or “High”) policy so that those computers require authorization for access. Ex. 1005, 1020 (“Authentication methods limit access from *unauthorized* users.” (emphasis added)), 1024 (“IPSec policies can be selected” on a “computer . . . [that] is connected to other hosts by means of an enterprise *intranet*.” (emphasis added)), 1025 (“Requires that all communications . . . be secured.”). Thus, because the corporate intranet DNS resolves domain names for those computers connected to the corporate intranet, the corporate intranet DNS returns addresses that require authorization for access. *Id.* at 989–990, 1020, 1024–1025, Fig. 22.12.

Patent Owner argues that “all of the DNS servers in Windows Resource Kit are conventional DNS servers that are not capable of resolving a non-standard domain name corresponding to a secure computer network address.” PO Resp. 38 (citing Ex. 2015 ¶ 64) (emphasis omitted). Patent Owner’s argument is not persuasive. As discussed above, Windows Resource Kit discloses a corporate intranet DNS that resolves domain names that cannot be resolved by a conventional public DNS. Ex. 1005, 971, 989 (“Client1 resolves intranet names by using a name server on the intranet, NoamDC1, and resolves Internet names by using a name server on the Internet, ISPName Server.”), 990, Figs. 22.4, 22.12. As also discussed above, Windows Resource Kit discloses that the corporate intranet DNS returns secure computer network addresses because it returns IP addresses for computers on the corporate intranet that require authorization for access. *Id.* at 989–990, 1020, 1024–1025, Fig. 22.12.

Patent Owner argues that Windows Resource Kit does not disclose a DNS that recognizes that a query is requesting a secure computer network address. PO Resp. 38 (citing Ex. 2015 ¶ 65). Patent Owner’s argument is not persuasive. Patent Owner does not explain specifically what it means for a DNS to recognize that a query is requesting a secure computer network address or why the corporate intranet DNS in Windows Resource Kit does not recognize that a query is requesting a secure computer network address. *See* PO Resp. 14–20, 38; Ex. 2015 ¶ 65. Moreover, the ’643 patent indicates that an SDNS “contains a cross-reference database of secure domain names and corresponding secure network addresses.” Ex. 1001, col. 51, ll. 6–7. As such, the SDNS described in the ’643 patent may recognize that a query is requesting a secure computer network address by comparing the domain

name in the query to the domain names in the database.³ *Id.* at col. 40, ll. 1–7 (“If access to a secure site has been requested (as determined, for example . . . by reference to an internal table of such sites).”), col. 51, ll. 6–13.

Windows Resource Kit discloses a corporate intranet DNS that includes a database of domain names and corresponding IP addresses for secure computers on a corporate intranet. Ex. 1005, 989 (“Client1 resolves intranet names by using a name server on the intranet, NoamDC1, and resolves Internet names by using a name server on the Internet, ISPName Server.”), 990, Fig. 22.12. Thus, like the SDNS in the ’643 patent, the corporate intranet DNS in Windows Resource Kit may recognize that a query is requesting a secure computer network address by comparing the domain name in the query to the domain names in the database. Ex. 1001, col. 40, ll. 1–7; Ex. 1005, 989–990, Fig. 22.12.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 7 and 22 are anticipated by Windows Resource Kit.

9. *Claims 8 and 23*

Claim 8 depends from claim 7, and recites “receiving the at least one network address in response to the query from the SDNS.” Ex. 1001, col.

³ At the oral hearing, Patent Owner argued that the SDNS in the ’643 patent recognizes that a query is requesting a secure computer network address based on the “.scom” top-level domain name. Tr. 51:10–52:3. Patent Owner’s argument is not persuasive. The ’643 patent states that the “.scom” top-level domain name is a non-limiting example. Ex. 1001, col. 50, ll. 25–29. Further, the ’643 patent indicates that the SDNS also can recognize that a query is requesting a secure computer network address by comparing the domain name in the query to the list of domain names in a table. *Id.* at col. 40, ll. 1–7.

56, ll. 24–26. Claim 23 depends from claim 22, and recites similar limitations. *Id.* at col. 57, ll. 60–63. Windows Resource Kit discloses a corporate intranet DNS that returns an IP address in response to a query for a domain name. Pet. 40; Ex. 1005, 989–990, Fig. 22.12. Further, as discussed above, the corporate intranet DNS is an SDNS. *See supra* Section II.B.8. Other than the arguments discussed above with respect to claims 7 and 22, Patent Owner does not dispute that Windows Resource Kit discloses the limitations of claims 8 and 23. PO Resp. 43.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 8 and 23 are anticipated by Windows Resource Kit.

10. *Claims 9 and 24*

Claim 9 depends from claim 7, and recites “receiving, in response to the query, a list of network addresses associated with the domain name.” Ex. 1001, col. 56, ll. 27–29. Claim 24 depends from claim 22, and recites similar limitations. *Id.* at col. 58, ll. 1–4. Windows Resource Kit discloses a corporate intranet DNS that returns multiple IP address in response to a query for a domain name. Pet. 40–41; Ex. 1003 ¶ 172, 174–175; Ex. 1005, 986, 989–990, Fig. 22.12. Further, as discussed above, the corporate intranet DNS is an SDNS. *See supra* Section II.B.8. Other than the arguments discussed above with respect to claims 7 and 22, Patent Owner does not dispute that Windows Resource Kit discloses the limitations of claims 9 and 24. PO Resp. 43.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 9 and 24 are anticipated by Windows Resource Kit.

11. *Claims 12 and 27*

Claim 12 depends from claim 1, and recites that “the identifier includes a non-secure domain name” and that “constructing the domain name includes replacing the non-secure domain name with a secure domain name.” Ex. 1001, col. 56, ll. 54–57. Claim 27 depends from claim 17, and recites similar limitations. *Id.* at col. 58, ll. 28–32.

Petitioner argues that a non-secure domain name is “a name that corresponds to a non-secure computer network address,” and a secure domain name is “a name that corresponds to a secure computer network address.” Pet. 12 (emphasis omitted). Patent Owner argues that a non-secure domain name is “a standard domain name that corresponds to a non-secure computer network address, i.e., a network address that does not require authorization for access, and can be resolved by a conventional domain name service (DNS),” and a secure domain name is “a non-standard domain name that corresponds to a secure computer network address, i.e., a network address that requires authorization for access, and cannot be resolved by a conventional domain name service (DNS).” PO Resp. 5. For the reasons discussed below, we determine that Petitioner has not shown sufficiently that Windows Resource Kit discloses the limitations of claims 12 and 27 under either proposed construction. Thus, we need not adopt either proposed construction to resolve the parties’ dispute regarding claims 12 and 27.

Petitioner argues that Windows Resource Kit discloses sending a query using a first domain name “client1.dom1.acquired01-int.com” to a DNS. Pet. 42 (citing Ex. 1003 ¶ 165; Ex. 1005, 976). According to Petitioner, the first domain name “can be either a secure or non-secure

domain name, depending on whether the primary DNS suffix that has been set can be resolved conventionally or not.” Pet. 42. Petitioner further argues that, if the query to the DNS using the first domain name fails to return an IP address, the first domain name is replaced with a second domain name “client1.acquired01-ext.com.” Pet. 42 (citing Ex. 1005, 976). According to Petitioner, the second domain name also “can either be a secure or non-secure domain name depending on whether the fully qualified domain name can be resolved conventionally.” Pet. 42–43.

Petitioner’s argument is not persuasive. Petitioner does not direct us to an express disclosure in Windows Resource Kit indicating that the first domain name “client1.dom1.acquired01-int.com” is a non-secure domain name, or that the second domain name “client1.acquired01-ext.com” is a secure domain name. *Id.* Petitioner also does not direct us to specific evidence indicating that a person of ordinary skill in the art would have at once envisaged that the first domain name is a non-secure domain name and the second domain name is a secure domain name. *Id.* Petitioner instead relies on attorney argument suggesting that it is possible that the first domain name could be a non-secure domain name and the second domain name could be a secure domain name. *Id.* That is not sufficient to show that Windows Resource Kit anticipates claims 12 and 27.

Petitioner also argues that Windows Resource Kit discloses a corporate intranet DNS that resolves intranet domain names, and a public DNS that resolves Internet domain names. Pet. 43 (citing Ex. 1005, 989–990). According to Petitioner, Windows Resource Kit discloses using a host name “coffee” to construct the domain names “coffee.com,” “coffee.reskit.com,” and “coffee.redmond.reskit.com.” Pet. 43–44 (citing

Ex. 1003 ¶¶ 168–170; Ex. 1005, 989–990) (emphasis omitted). Petitioner argues that “[t]he intranet DNS server will not resolve the non-secure (public) domain name coffee.com, but will resolve the secure (private) domain name coffee.reskit.com or coffee.redmond.reskit.com.” Pet. 44 (emphasis omitted).

Petitioner’s argument is not persuasive. We agree that Windows Resource Kit discloses a corporate intranet DNS that resolves corporate intranet domain names, and a public DNS that resolves Internet domain names. *See supra* Section II.B.8. Petitioner, however, does not direct us to an express disclosure in Windows Resource Kit indicating that “coffee.com” is a public domain name that the corporate intranet DNS will not resolve, or that “coffee.reskit.com” and “coffee.redmond.reskit.com” are private domain names that the corporate intranet will resolve. Pet. 43–44; Ex. 1003 ¶¶ 168–170. Petitioner also does not direct us to specific evidence indicating that a person of ordinary skill in the art would have at once envisaged that scenario. *Id.* Petitioner instead relies on attorney argument suggesting that it is possible that “coffee.com” is a public domain name that the corporate intranet DNS will not resolve, and that it is possible that “coffee.reskit.com” and “coffee.redmond.reskit.com” are private domain names that the corporate intranet will resolve. Pet. 44. That is not sufficient to show that Windows Resource Kit anticipates claims 12 and 27.

Therefore, we determine that Petitioner has not shown by a preponderance of the evidence that claims 12 and 27 are anticipated by Windows Resource Kit.

12. *Claims 14 and 29*

Claim 14 depends from claim 1, and recites “wherein the encrypted communication link comprises a virtual private network communication link over the communication network.” Ex. 1001, col. 57, ll. 3–5. Claim 29 depends from claim 17, and recites similar limitations. *Id.* at col. 58, ll. 46–48. Windows Resource Kit discloses creating a private communication path between computers using, *inter alia*, encryption and authentication techniques. Pet. 44; Ex. 1003 ¶¶ 182–184; Ex. 1005, 1019–1021. Patent Owner does not dispute that Windows Resource Kit discloses the above limitations of claims 14 and 29.

Therefore, we determine that Petitioner has shown by a preponderance of the evidence that claims 14 and 29 are anticipated by Windows Resource Kit.

13. *Petitioner’s Reliance on Additional Documents*

Patent Owner argues that Petitioner improperly relies on documents other than Windows Resource Kit to disclose certain limitations in the challenged claims. PO Resp. 43–48. Specifically, Patent Owner contends that “throughout the Petition, Petitioner repeatedly cites to and relies upon its declarant’s testimony, which, in turn, cites to numerous additional references not disclosed to be part of Windows Resource Kit.” *Id.* at 43–44 (emphasis omitted). According to Patent Owner, these citations “operate to obscure which references and which portion of which reference discloses the claim limitation.” *Id.* at 44. Patent Owner’s argument is not persuasive. For the reasons discussed above, Petitioner has shown sufficiently that Windows Resource Kit *alone* discloses the limitations of claims 1–9, 14, 17–24, and 29 of the ’643 patent. *See supra* Sections II.B.2–II.B.12. Any

discussion of additional documents by Petitioner's declarant, Dr. Roberto Tamassia, does not obscure our ability to determine that claims 1–9, 14, 17–24, and 29 are anticipated by Windows Resource Kit. *See id.*

Patent Owner also argues that the additional documents discussed by Dr. Tamassia demonstrate that Windows Resource Kit does not disclose a first device that receives encrypted communication link resources from a server that is separate from the first device. PO Resp. 47–48. Patent Owner acknowledges that Windows Resource Kit discloses two computers that exchange public keys. *Id.* at 47. Patent Owner argues, though, that the additional documents discussed by Dr. Tamassia indicate that the exchange also may be performed through a third party device, and, thus, the first computer does not necessarily receive the public key from the second computer. *Id.* at 47 (citing Ex. 1003 ¶¶ 123, 126). Patent Owner's argument is not persuasive. Figure 22.19 of Windows Resource Kit expressly shows that the first computer receives a public key from the second computer, and Patent Owner does not dispute that the second computer is a server separate from the first computer. Ex. 1005, 1021–1022, 1025, Fig. 22.19. Thus, regardless of whether other documents indicate that the exchange also may be performed in a different manner, Windows Resource Kit *alone* discloses receiving encrypted communication link resources from a server that is separate from the first device. *Id.*

C. *Obviousness of Claims 1, 13, 15–17, 28, and 30–32 over Windows Resource Kit, IE5 Resource Kit, and Elgamal*

Petitioner argues that claims 1, 13, 15–17, 28, and 30–32 would have been obvious over Windows Resource Kit, IE5 Resource Kit, and Elgamal. 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, 13, 15–17, 28, and 30–32 would have been obvious over Windows Resource Kit, IE5 Resource Kit, and Elgamal.⁴

1. *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

⁴ This determination is not inconsistent with our determination above that Petitioner has shown by a preponderance of the evidence that independent claims 1 and 17 are anticipated by Windows Resource Kit. Petitioner suggests that IE5 Resource Kit and Elgamal are included in this asserted ground of unpatentability just to teach the limitations in dependent claims 13, 15, 16, 28, and 30–32. See Pet. 45. Petitioner, however, also changes the theory of unpatentability for independent claims 1 and 17 by relying on Elgamal, rather than Windows Resource Kit, to teach enabling a secure communication mode. Compare *id.* at 20–22, with *id.* at 48–49.

second device.” *Id.* at col. 55, ll. 52–58. Petitioner relies on Elgamal to teach enabling a secure communication mode. Pet. 49. Specifically, Petitioner argues that Elgamal teaches enabling a Secure Sockets Layer (“SSL”) secure communication mode by clicking a link in a browser. *Id.* (citing Ex. 1003 ¶¶ 221–223; Ex. 1007, col. 9, ll. 32–41). Petitioner relies on Windows Resource Kit to teach constructing a domain name. Pet. 23–27, 50. Specifically, Petitioner argues that Windows Resource Kit teaches constructing a domain name by adding a suffix to a host name to create a fully qualified domain name. *Id.* (citing Ex. 1003 ¶¶ 162–170; Ex. 1005, 967–968, 972, 976–977).

Patent Owner contends that combining the cited teachings in Windows Resource Kit and Elgamal would not result in the method recited in claim 1 of the ’643 patent. PO Resp. 49–51 (citing Ex. 2015 ¶¶ 75–79). 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 Windows Resource Kit teaches constructing a domain name by adding a suffix to a host name to create a fully qualified domain name (Pet. 23–27, 50). Elgamal teaches, though, that when a user clicks on a link to enable an SSL secure communication mode, that link already includes a fully qualified domain name that points to a particular document or other resource. Ex. 1007, col. 9, ll. 32–38, col. 14, ll. 16–22; Ex. 2015 ¶ 78. Because the link in Elgamal already includes a fully qualified domain name, the cited feature in Windows Resource Kit would not add a suffix to the

name in the link, and, thus, would not construct a domain name. Ex. 2015 ¶ 79. Petitioner does not dispute this point.⁵ See Pet. Reply 18–20.

Petitioner instead argues in the Reply that Windows Resource Kit also “discloses **removing** a portion of a DNS suffix.” Pet. Reply 19 (citing Ex. 1005, 977). Petitioner’s argument is not persuasive. As discussed above, Elgamal teaches that the link for enabling an SSL secure communication mode already includes a fully qualified domain name that points to a particular document or other resource. Ex. 1007, col. 9, ll. 32–38, col. 14, ll. 16–22; Ex. 2015 ¶ 78. Petitioner does not provide a specific reason why it would have been obvious to a person of ordinary skill to combine the identified prior art so that the cited feature in Windows Resource Kit removes a portion of the name in the link in Elgamal. See Pet. 23–27, 47–50; Pet. Reply 18–20.

Petitioner also argues in the Reply that an SSL secure communication mode can be enabled by a user typing a domain name in a browser, not just by clicking on a link. Pet. Reply 20. Specifically, Petitioner argues as follows:

Instead, Patent Owner effectively assumes that all URLs in the combined system must be “fully qualified domain name[s]” because Elgamal only describes “a user ‘click[ing]’” a URL. Resp., 50; Ex. 2015, ¶78. Patent Owner’s rationale is remarkable—that because Elgamal does not literally disclose a user typing out a domain name, enabling SSL in Internet Explorer 5 on Windows 2000 would somehow prevent a user from typing out a domain name. This contention has no basis in

⁵ Petitioner also does not argue specifically or identify specific evidence indicating that it would have been obvious to modify the link in Elgamal in some way so that the cited feature in Windows Resource Kit would add a suffix to the name in the link. See Pet. 47–50; Pet. Reply 18–20.

the evidence or the understanding of an ordinary artisan. Ex. 1003, ¶¶267–69. Patent Owner’s argument should thus be dismissed.

Pet. Reply 20 (emphasis omitted). Petitioner’s argument is not persuasive. Petitioner does not direct us to any specific portion of Elgamal that teaches enabling an SSL secure communication mode by typing a domain name in a browser. *See id.* In addition, the declaration testimony cited by Petitioner does not indicate that a person of ordinary skill in the art otherwise would have known that an SSL secure communication mode can be enabled by typing a domain name in a browser. *See* Ex. 1003 ¶¶ 267–269. As a result, Petitioner relies on attorney argument, which is not sufficient to show that a claim limitation would have been obvious.

Moreover, 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 Elgamal teaches enabling an SSL secure communication mode by clicking a link in a browser. Pet. 49 (citing Ex. 1003 ¶¶ 221–223; Ex. 1007, col. 9, ll. 32–41). Petitioner does not argue specifically in the Petition that Windows Resource Kit, IE5 Resource Kit, or Elgamal teaches or suggests enabling an SSL secure communication mode by typing a domain name in a browser. *See* Pet. 49. 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).

For the foregoing reasons, Petitioner has not shown sufficiently that the combination of Windows Resource Kit, IE5 Resource Kit, and Elgamal

teaches the limitations in claim 1. Therefore, we determine that Petitioner has not shown by a preponderance of the evidence that claim 1 would have been obvious over Windows Resource Kit, IE5 Resource Kit, and Elgamal.

2. *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 identifier 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 1.⁶ Pet. 48–52. 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 Windows Resource Kit, IE5 Resource Kit, and Elgamal. *See supra* Section II.C.1.

3. *Claims 13, 15, 16, 28, 30, 31, 32*

Claims 13, 15, 16, 28, and 30–32 depend 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 13, 15, 16, 28, and 30–32 would have been obvious over Windows Resource Kit, IE5 Resource Kit, and Elgamal. *See supra* Sections II.C.1–II.C.2.

⁶ Neither party argues that claim 17 should be treated differently than claim 1 because it is a system claim.

D. *Declaration of Dr. Roberto Tamassia*

Patent Owner argues that the testimony of Petitioner's declarant, Dr. Tamassia, should be given little, if any, weight because Dr. Tamassia "never explains in any detail how each claim element is disclosed, taught, or suggested by the references." PO Resp. 57. Patent Owner's argument is not persuasive. As demonstrated by the discussion and citations above, Petitioner identifies in the Petition which specific portions of the prior art disclose or teach each limitation of the challenged claims, and Petitioner relies on Dr. Tamassia's testimony to explain those portions of the prior art in further detail. *See supra* Sections II.B–II.C. Dr. Tamassia does not provide a direct comparison of each limitation in the challenged claims to the prior art, but his testimony nonetheless is helpful to us in understanding the scope and content of the prior art cited in the Petition. *See* Fed. R. Evid. 702; *Graham*, 383 U.S. at 17–18.

Patent Owner cites to *Schumer v. Laboratory Computer Systems, Inc.*, 308 F.3d 1304 (Fed. Cir. 2002), to support its argument. PO Resp. 56–57. *Schumer* states that expert testimony "[t]ypically . . . must identify each claim element, state the witnesses' interpretation of the claim element, and explain in detail how each claim element is disclosed in the prior art reference," but *Schumer* does not require us to discount expert testimony just because it does not address each of those items. 308 F.3d at 1315–16 (emphasis added). Rather, *Schumer* explains more broadly that it is improper to accept "conclusory," "confusing," or "generalized" testimony. *Id.*; *see also Koito Mfg. v. Turn-Key-Tech, LLC*, 381 F.3d 1142, 1152 (Fed. Cir. 2004) ("General and conclusory testimony, such as that provided by Dr. Kazmer in this case, does not suffice as substantial evidence of invalidity.").

Here, Patent Owner does not identify any portions of Dr. Tamassia's testimony that are conclusory, confusing, or generalized. And, based on our review of the record, we do not find Dr. Tamassia's testimony to be conclusory, confusing, or generalized.

E. *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 1004, 1021–1023, 1025–1031, 1034, and 1040–1044, 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*.

1. *Exhibits 1004, 1021–1023, 1025–1031, 1034, and 1040–1044*

Patent Owner argues that Exhibits 1004, 1021–1023, 1025–1031, 1034, and 1040–1044 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. 2. 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 1004, 1021–1023, 1025–1031, 1034, and 1040–1044 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. 2–3. 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*.

III. CONCLUSION

Petitioner has shown by a preponderance of the evidence that claims 1–9, 14, 17–24, and 29 of the ’643 patent are unpatentable. Petitioner, however, has not shown by a preponderance of the evidence that claims 12, 13, 15, 16, 27, 28, and 30–32 are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–9, 14, 17–24, and 29 of the ’643 patent are shown unpatentable;

FURTHER ORDERED that claims 12, 13, 15, 16, 27, 28, and 30–32 of the ’643 patent are not shown unpatentable;

FURTHER ORDERED that Patent Owner’s Motion to Exclude is *denied*; and

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.

IPR2015-01009
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