UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/333,605	12/21/2011	Matthew Mulder	087762-000153CIP1	7972

70001 7590 09/22/2020
NIXON PEABODY LLP
70 WEST MADISON STREET
SUITE 3500
CHICAGO, IL 60602

EXAMINER	
HUYNH, THU V	

ART UNIT	PAPER NUMBER
2177	

NOTIFICATION DATE	DELIVERY MODE
09/22/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketingchicago@nixonpeabody.com
ipairlink@nixonpeabody.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte MATTHEW MULDER and JOHN SAFA

Appeal 2019-000054
Application 13/333,605
Technology Center 2100

Before JOHN P. PINKERTON, CARL L. SILVERMAN, and JASON M. REPKO, *Administrative Patent Judges*.

PINKERTON, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–31, which are all of the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies Workshare, Ltd. as the real party in interest. Appeal Br. 2.

STATEMENT OF THE CASE

Introduction

Appellant generally describes the disclosed and claimed invention as providing "a mechanism whereby a group of people operating individual computer devices can view and share and collaboratively edit an electronic document stored in a remote data repository." Spec. ¶ 2.[2]

Claim 1 is the only independent claim and is reproduced below (with formatting changes added):

> 1. A computer system for providing access to documents comprised of:
>
> a first server comprised of a first computer memory device, said first computer memory device comprised of data embodying a document
>
> a second server in communication by a data network with said first server and in further communication with a remote device,
>
> said remote device further comprised of a receiving module adapted by logic to receive from the second server data representing directory listings comprised of a data referencing a document,
>
> a first transmitting module adapted by logic to transmit to the second server a data message containing a request comprised of the reference to the document,

[2] Our Decision refers to the Final Office Action mailed Sept. 21, 2017 ("Final Act."); the Appeal Brief filed May 8, 2018 ("Appeal Br."); the Examiner's Answer mailed July 27, 2018 ("Ans."); the Reply Brief filed Sept. 27, 2019 ("Reply Br."); and the original Specification filed Dec. 21, 2011 ("Spec."). The pages of the Appeal Brief and the Reply Brief are not numbered. We consider the title page of each brief to be numbered page 1 and the following pages to be numbered consecutively thereafter.

> said second server being comprised of an authentication module adapted by logic to authenticate the request received from the remote device by executing a first security protocol between the remote device and the second server to determine a first authenticated logic state associated with the received document request and in response to the first authenticated logic state, execute a second security protocol between the first server and the second server to determine a second authenticated logic state for the received document request, and
>
> in response to the second authenticated logic state, transmit to the first server a request for the referenced document, where the first server is further comprised of a second transmitting module adapted by logic to transmit the referenced document to the second server.

Appeal Br. 23 (Claims App.).

References

Name	Patent or Publication Number	Date
Skarbo et al. ("Skarbo")	US 6,317,777 B1	Nov. 13, 2001
Teugels et al. ("Teugels")	US 7,958,101 B1	June 7, 2011
Zilka	US 8,117,225 B1	Feb. 14, 2012
Felsher et al. ("Felsher")	US 8,316,237 B1	Nov. 20, 2012
Cavage et al. ("Cavage")	US 8,776,190 B1	July 8, 2014
Saether et al. ("Saether")	US 2001/0042073 A1	Nov. 15, 2001
Sharif et al. ("Sharif")	US 2003/0009528 A1	Jan. 9, 2003
Yoshida et al. ("Yoshida")	US 2006/0277229 A1	Dec. 7, 2006
Zhang	US 2007/0179967 A1	Aug. 2, 2007
Saito	US 2009/0319480 A1	Dec. 24, 2009

Ravi et al. (“Ravi”)	US 2010/0064004 A1	Mar. 11, 2010
Egnor	US 2010/0076985 A1	Mar. 25, 2010
Sharma et al. (“Sharma”)	US 2010/0174826 A1	July 8, 2010
Heineken	US 2011/0035655 A1	Feb. 10, 2011
Park	US 2011/0125806 A1	May 26, 2011
Hebbar et al. (“Hebbar”)	US 2014/0032489 A1	Jan. 30, 2014

Rejections on Appeal[3]

Claims 1, 3–5, 8, 13, 14–17, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, and Felsher.

Claims 2 and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, Cavage, and Park.

Claims 6, 7, 9, and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Saether.

Claims 11 and 12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, Saether, Egnor, and Heineken.

Claims 18 and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Zilka.

Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Zhang.

[3] The Examiner rejected claims 1–31 under 35 U.S.C. § 101 because the system of claim 1 “appears to be software per se,” which is not statutory subject matter. Final Act. 3. However, the Examiner subsequently withdrew this rejection. Ans. 19.

Claim 21 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Yoshida.

Claims 23–25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, Ravi, Skarbo, and Zilka.

Claim 28 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Hebbar.

Claims 29–31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, Felsher, and Sharif.

ANALYSIS

The dispositive issue raised by the arguments in Appellant's briefs is whether the combination of Teugels, Sharma, Saito, and Felsher teaches or suggests the limitation, in response to the first authenticated logic state, "execute a second security protocol between the first server and the second server to determine a second authenticated logic state for the received document request," as recited in claim 1 (hereinafter, "the disputed limitation").

The Examiner rejected independent claim 1 under 35 U.S.C. § 103(a) as being unpatentable over Teugels, Sharma, Saito, and Felsher. Final Act. 2–4. The Examiner finds that Teugels's disclosure of content addressable storage ("CAS") system 509 that stores a plurality of content units teaches "a first server comprised of a first computer memory device, said first computer memory device comprised of data embodying a document." Final Act. 4 (citing Teugels, Fig. 5B); Ans. 22 (citing Teugels 10:12–13, 10:48–49). The Examiner also finds that Teugels's disclosure of appliance 517 in communication by a data network with CAS system 509 and in further communication with user device 501 teaches "a second server in communication by a data network with said first server and in further communication with a remote device." Ans. 22 (citing Teugels 11:31–58).

The Examiner further finds that Teugels does not teach

> the second server being comprised of an authentication module adapted by logic to authenticate the request received from the remote device by executing a first security protocol between the remote device and the second server to determine a first authenticated logic state associated with the received document request; and in response to the first authenticated logic state, *execute second security protocol between the first server and the second server to determine a second authenticated logic state for the received document request.*

Final Act. 5 (emphasis added). With respect to these limitations, the Examiner finds that Sharma's disclosure of network server 103 teaches "second server being comprised of an authentication module" to authenticate a document request from a client and, if the request is valid, determine if the type of document request is authorized. Final Act. 5 (citing Sharma, Figs. 1, 2; ¶¶ 31–36). The Examiner also finds that Saito teaches "second server being comprised of an authentication module" to execute a first security protocol between the remote device and the second server. *Id.* at 6 (citing Saito, Fig. 7; ¶ 94 ("server 30")). The Examiner further finds that Felsher teaches "authentication between parties to ensure . . . each of the parties is [the] intended party to communicate/send data" and, therefore, Felsher teaches "second security protocol between the first server and the second server." *Id.* (citing Felsher, Fig. 3; 28:30–45); Ans. 26 (citing Felsher, Fig. 3; 28:30–45; 29:3–6). Moreover, the Examiner finds that "the combination of Felsher, Sharma, and Teugels teaches authentication between servers to verify intended parties/servers." Ans. 26 (emphasis omitted) (citing Felsher 29:3–6).

In response to Appellant's arguments that "Sharma does not disclose a security protocol . . . conducted between a 'first server' and "second server' as claimed" (*see* Appeal Br. 14–16), the Examiner, in the Answer, relies on Figure 3 of Sharma, in addition to Figure 1, and finds that Sharma's disclosure of application server 301 in communication with "Web server 305, which similar to the network server 103 of Fig. 1 performs security processing via a digital certificate authenticator 306 for performing a first security procedure" (emphasis omitted) teaches "second server . . . comprised of an authentication module adapted by logic to authenticate the request received from the remote device by executing a first security protocol." Ans. 23–24 (citing Sharma, Fig. 3; ¶ 41). The Examiner also finds that Sharma's disclosure of application server 301 in communication with Web server 305, which performs security processing via a "so-called SiteMinder agent 307 [and Policy Server] for performing a second security procedure" teaches in response to the first authenticated logic state "execute second security protocol to determine a second authenticated logic state for the document request." *Id.* at 24–25 (citing Sharma ¶¶ 31–33, 41).

In the Appeal Brief, Appellant argues that Sharma fails to disclose "execute a second security protocol between the first server and the second server to determine a second authenticated logic state" because "Sharma's second security test is performed by the 'policy server"—as is the first security test." Appeal Br. 15–16. In response to this argument, the Examiner states that, as explained, Sharma teaches "first security protocol (using digital certificate authenticator 306) and second security protocol (SiteMinder Agent 307 and Policy Server)." Ans. 25. The Examiner then states that "[b]esides using digital certificate authenticator 306 to authenticate user request to verify exchange of information is permitted," Sharma teaches application server 301[4] has a "module to perform 'Digital Certificate Manager' function." *Id.* at 25–26 (citing Sharma, Fig. 3, ¶ 37). However, the Examiner acknowledges that "Sharma does not explicitly describe how the Digital Certificate Manager function authenticate[s] between first server 301 and second server 305." *Id.* at 26.

Appellant argues that the '"Network file server' of Teugels and the 'CAS System' are all components of the same server with one file system-- they are not two logically distinct servers, that is, they do not disclose the 'first server' and 'second server' as recited in Appellant's claims." Appeal Br. 11–13; Reply Br. 2–4. Appellant also argues that Sharma fails to disclose "that a 'request' is passed to a 'second security protocol between the first server and the second server to determine a second authenticated logic state"' because "Sharma's second security test is performed by the 'policy server'—as is the first security test." Appeal Br. 15 (citing Sharma, Fig. 2). Appellant further argues that neither Felsher nor Saito disclose a security protocol between the first server and second server as claimed. *Id.* at 16–19.

We are persuaded by Appellant's arguments that the Examiner erred. Even assuming that Teugels's disclosure of CAS system 509 teaches the claimed "first server" and that Teugels's disclosure of appliance 517 in communication by a data network with CAS system 509, and in further communication with user device 501, teaches the claimed "second server,"

[4] The Examiner refers to "application server 310," but we believe this is a mistake because, in Sharma's Figure 3, the application server is designated 301 and no component is designated as 310. Ans. 25.

we find the Examiner has not demonstrated by a preponderance of the evidence that the combination of Teugels, Sharma, Felsher, and Saito teaches or suggests the disputed limitation.

First, the Examiner fails to demonstrate that application server 105 in communication with network server 103, as shown in Figure 1 of Sharma, or that application server 301 in communication with web server 305, as shown in Figure 3 of Sharma, teaches or suggests the disputed limitation because, as Appellant argues, "Sharma's second security test is performed by the 'policy server'—as is the first security test." Appeal Br. 15. Regarding Figure 1, Sharma discloses authenticating a request for information on a particular user from the external aggregator 101 in a two-step process. In the first check, Sharma discloses that network server 103 "sends the digital certificate [from the external aggregator] to the policy server 113" to determine whether the external aggregator is a valid or authorized requester. Sharma ¶ 31. In an optional second security check to determine if the type of information requested is the type the user is authorized to access, Sharma discloses that the user's credentials are "forwarded from the network server 103 to the policy server 113, which verifies whether the user is permitted to access the type of information requested." Sharma ¶ 32. Thus, we agree with Appellant's argument that the application server of Sharma "does no authentication," but is passed a request at step 208 of Figure 2 that has already been authenticated with respect to the type of information requested at step 206 by the "policy server." Appeal Br. 16. Similarly, in regard to Figure 3, Sharma discloses that application server 301 is in communication with web server 305, which, similar to the network server 103 of Fig. 1, performs security processing . . . *as discussed above*." Sharma ¶ 41 (emphasis added). Figure 3 depicts SiteMinder Policy Server in communication with web server 305. Thus, like application server 105 in Figure 1, application server 301 in Figure 3 does no authentication, but is passed a request that has been authenticated by the "policy server."

Second, as discussed above, in response to Appellant's arguments that Sharma's security authentication is performed by the policy server, rather than the application servers, the Examiner further finds that Sharma's application server 301 includes a "module to perform 'Digital Certificate Manager' function." Ans. 25–26 (citing Sharma, Fig. 3, ¶ 37). This finding is unsupported and unconvincing, however, because as mentioned above, the Examiner specifically acknowledges that "Sharma does not explicitly describe how the Digital Certificate Manager function authenticates between first server 301 and second server 305." *Id.* at 26.

Third, with respect to Felsher and Saito, for the reasons stated by Appellant, we determine the Examiner has not provided persuasive evidence or technical reasoning demonstrating that either Felsher or Saito teaches or suggests "execute a second security protocol between the first server and the second server to determine a second authenticated logic state for the received document request," as recited in claim 1. *See* Appeal Br. 16–19. We also fail to discern how either Felsher or Saito teaches or suggests the disputed limitation. Thus, we determine that the Examiner has failed to show that the combination of Teugels, Sharma, Felsher, and Saito teaches or suggests the disputed limitation of claim 1.

In view of the foregoing, we do not sustain the Examiner's rejection of independent claim 1 under 35 U.S.C. § 103(a). For the same reasons, we do not sustain the Examiner's rejection of dependent claims 2–31. *Cf. In re*

Fritch, 972 F.2d 1260, 1266 (Fed. Cir. 1992) ("[D]ependent claims are nonobvious if the independent claims from which they depend are nonobvious").

DECISION

We reverse the Examiner's rejection of claims 1–31 under 35 U.S.C. § 103(a).

SUMMARY

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/Basis	Affirmed	Reversed
1, 3–5, 8, 13, 14–17, 22	103(a)	Teugels, Sharma, Saito, Felsher		1, 3–5, 8, 13, 14–17, 22
2, 27	103(a)	Teugels, Sharma, Saito, Felsher, Cavage, Park		2, 27
6, 7, 9, 10	103(a)	Teugels, Sharma, Saito, Felsher, Saether		6, 7, 9, 10
11, 12	103(a)	Teugels, Sharma, Saito, Felsher, Saether, Egnor, Heineken		11, 12
18, 26	103(a)	Teugels, Sharma, Saito, Felsher, Zilka		18, 26
19	103(a)	Teugels, Sharma, Saito, Felsher, Zhang		19
21	103(a)	Teugels, Sharma, Saito, Felsher, Yoshida		21
23–25	103(a)	Teugels, Sharma, Saito, Felsher, Ravi, Skarbo, Zilka		23–25

28	103(a)	Teugels, Sharma, Saito, Felsher, Hebbar		28
29–31	103(a)	Teugels, Sharma, Saito, Felsher, Sharif		29–31
Overall Outcome				1–31

<u>REVERSED</u>