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.
12/943,428	11/10/2010	Gordon Yong LI	2875.3420003	3647

49579 7590 10/31/2016
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER
AGUIAR, JOHNNY B

ART UNIT	PAPER NUMBER
2447	

MAIL DATE	DELIVERY MODE
10/31/2016	PAPER

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.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte GORDON YONG LI, VICTOR T. HOU, and XUEMIN CHEN

Appeal 2014-007611
Application 12/943,428
Technology Center 2400

Before CAROLYN D. THOMAS, JAMES R. HUGHES, and MONICA S. ULLAGADDI, *Administrative Patent Judges*.

THOMAS, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants seek our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 15–22. Claims 1–14 are allowed. We have jurisdiction over the appeal under 35 U.S.C. § 6(b).

We AFFIRM.

The present invention relates generally to security integration between a wireless and a wired network. *See* Spec. ¶ 2.

Claims 15, 17, and 18 are illustrative:

15. A method in a wireless device to authenticate to a wireless service provider and a PacketCable service provider using a wireless gateway, comprising:

transmitting a single authentication credential to the wireless gateway;

receiving an authentication response from the wireless gateway; and

generating a shared secret to create a secure channel with the wireless gateway;

wherein the single authentication credential is configured to be used by the wireless gateway to authenticate the wireless device to both the wireless service provider and the PacketCable service provider.

17. The method of claim 15, the generating step comprising generating a session key using the shared secret to create the secure channel.

18. A method in an authentication server to authenticate a wireless device for both wireless service and a PacketCable service, comprising:

receiving a single authentication credential from a wireless gateway;

verifying the single authentication credential;

transmitting a response to the wireless gateway indicating a result of the verifying step; and

generating a shared secret if the verification of the single authentication credential is successful;

wherein the single authentication credential is used to authenticate the wireless device for both the wireless service and the PacketCable service.

Appellants appeal the following rejections:

R1. Claims 15 and 16 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan (US 2007/0140195 A1, June 21, 2007) and Nessett (US 6,766,453 B1, July 20, 2004);

R2. Claim 17 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan, Nessett, and Morais (US 2008/0177997 A1, July 24, 2008);

R3. Claims 18 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan and Narayanan (US 2008/0040606 A1, Feb. 14, 2008);

R4. Claim 19 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan, Narayanan, and Ansari (US 2010/0217837 A1, Aug. 26, 2010);

R5. Claim 20 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan, Narayanan, and Nagaraja (US 2009/0319771 A1, Dec. 24, 2009); and

R6. Claim 21 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Kaftan, Narayanan, and Morais.

ANALYSIS

Claims 15, 16, and 18–22

Issue 1: Did the Examiner err in finding that the combined teachings of Kaftan and Nessett, particularly Kaftan, teaches or suggests a single authentication credential is configured to be used . . . to authenticate the wireless device to both the wireless service provider and the PacketCable service provider?

Appellants contend "[t]he applied Kaftan reference describes ***authorization*** as opposed to ***authentication***. Therefore, Kaftan fails to teach at least . . . a single ***authentication*** credential. . . . authentication and

authorization are different" (App. Br. 13–14). Appellants further contend that "Nesset fails to remedy the deficiencies of Kaftan" (*id.* at 14).

In response, the Examiner finds that "Kaftan discloses authentication of a communication device . . . 'authorization' and 'authentication' have the same meaning in the Kaftan reference because both terms are used interchangeably" (Ans. 10, *citing* Kaftan ¶¶ 24 and 26). We agree with the Examiner.

Specifically, Kaftan discloses "a Wireless Access Point system for use in a hybrid wireless/cable network, the system capable of *authenticating* a communication device (mobile and non-mobile) via DOCSIS and/or DOCSIS-compatible protocol and providing the IP service to the mobile device in accordance with a result of the *authentication*" (¶ 24; see also ¶ 26 and Abstract) (emphasis added). Although, as identified by Appellants, Kaftan also uses the term "authorized" (*see* ¶ 60), we agree with the Examiner that there is ample evidence in Kaftan that "authentication" of the mobile device also takes place.

Appellants further contend that "[j]ust because Kaftan describes PacketCable services in paragraph [0047] does not imply that the mobile device is authenticated (or even authorized) for use of ***both*** IP and PacketCable services when it is authorized for use of IP services" (App. Br. 15) and "Kaftan describes authorizing for an IP service and not necessarily a wireless service" (*id.* at 16).

In response, the Examiner finds "Kaftan discloses a single authentication credential (unique MAC address, see page 5 [0056]) of a wireless device . . . the unique MAC address is used to authenticate the mobile device to receive an IP service . . . and the IP service is provided by

either a wireless network . . . and/or a PacketCable network" (Ans. 9). We agree with the Examiner.

For example, Kaftan discloses "a Wireless Access Point system for use in a hybrid wireless/cable network" (*see* Abstract) and that a virtual cable modem is able to receive a request for an IP service from a mobile device thru the Wireless Access Point (e.g. WiMAX) and recognize a unique MAC address of the mobile device, convert the received address into a DOCSIS MAC, and forward the recognized MAC address as if it is a MAC address of the VCM (*see* ¶¶ 54–60). Kaftan further discloses that "[t]he term 'IP services' used in this patent specification should be expansively construed to cover any kind of communication services (e.g., data, video, voice, messaging, multi-media applications, etc.) delivering in association with IP packets" (¶ 39).

In other words, Kaftan's mobile device is authenticated using the unique MAC address for both the wireless service provider (i.e., WiMAX) and the PacketCable service provider (e.g., DOCSIS) and the IP services can include any kind of communication services (*see* Kaftan's Fig. 4).

Although Appellants direct our attention to paragraph [0022] of their Specification and emphasize in their arguments: "***It is a feature of the embodiments presented herein that second authentication credential 212 can authenticate wireless device 102 <u>simultaneously</u> for <u>both</u> . . .***" (*see* App. Br. 15), we note that Appellants' claims do not require that this process be done simultaneously, only that "a single authentication credential" be configured to be used by both the wireless service provider and the PacketCable service provider. We find that the claimed "single authentication credential" *reads on* Kaftan's "unique MAC address."

Appellants also contend that "[t]he Examiner has provided no required rationale underpinning for the conclusory statements of obviousness . . . rely on speculation, conjecture, and improper interpretation of both the claims and the applied references" (App. Br. 17).

Here, the Examiner finds that "[o]ne of ordinary skill in the art would be motivated to utilize the teachings of Nessett in the Kaftan system in order to efficiently avoid man-in-the-middle attacks" (Ans. 12). As noted *supra*, the Examiner has found actual teachings in the prior art and has provided the aforementioned rationale for the combination. Further, we find that the teachings suggest that the combination involves the predictable use of prior art elements according to their established functions. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007). Accordingly, we find that the Examiner has provided sufficient motivation for modifying Kaftan with the teachings of Nessett.

Accordingly, we sustain the Examiner's rejection of claims 15, 16, and claims 18–22 for similar reasons.

Claim 17

Issue 2: Did the Examiner err in finding that Morais teaches or suggests generating a session key using the shared secret, as set forth in claim 17?

The Examiner finds that "Morais teaches generating a session key . . . using the shared secret (Diffie-Hellman value . . .) to create the secure channel" (Ans. 12, *citing* Morais ¶¶ 76 and 79). Although Appellants contend "the applied portion of Morais fails to teach that the keys are generated in the same manner . . . using the ***shared secret*** to generate the

session key" (App. Br. 20), Appellants fail to distinguish Morais' "Diffie-Hellman value" (i.e., the Examiner's proffered "shared secret") from the claimed shared secret. Stated differently, the Examiner equates Morais' "Diffie-Hellman value" to the claimed "shared secret," and finds that such Diffie-Hellman value is used in Morais to generate security association keys. However, on this record, we find Appellants have failed to present *substantive* arguments and supporting *evidence* persuasive of Examiner error regarding the aforementioned disputed limitation. *See In re Lovin*, 652 F.3d 1349, 1357 (Fed. Cir. 2011)("we hold that the Board reasonably interpreted Rule 41.37 to require more substantive arguments in an appeal brief than a mere recitation of the claim elements and a naked assertion that the corresponding elements were not found in the prior art."). In other words, Appellants fail to provide any meaningful analysis as to *why* Morais fails to teach that it is known to use a shared secret to generate a key.

As such, we decline to examine the claims *sua sponte*, looking for distinctions over the prior art. *Cf. In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991) ("It is not the function of this court to examine the claims in greater detail than argued by an appellant, looking for [patentable] distinctions over the prior art."). *See also Ex parte Belinne*, No. 2009-004693, 2009 WL 2477843 at *3–4 (BPAI Aug. 10, 2009) (informative).

Accordingly, we sustain the Examiner's rejection of claim 17.

DECISION

We affirm the Examiner's § 103(a) rejections R1–R6.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED