



# 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.
12/509,794	07/27/2009	Richard Petillo	Y2108-00466	1745
39290	7590	11/22/2016	EXAMINER	
DUANE MORRIS LLP - DC			SALEHI, HELAI	
505 9th Street			ART UNIT	
Suite 1000			PAPER NUMBER	
WASHINGTON, DC 20004-2166			2433	
			MAIL DATE	
			DELIVERY MODE	
			11/22/2016	
			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* Richard PETILLO

---

Appeal 2015-007598  
Application 12/509,794  
Technology Center 2400

---

Before THU A. DANG, NORMAN H. BEAMER,  
and SCOTT E. BAIN, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–16.<sup>1</sup> We have jurisdiction over the pending rejected claims under 35 U.S.C. § 6(b).

We reverse.

---

<sup>1</sup> Appellant identifies Vonage Holdings Corporation as the real party in interest. (App. Br. 1.)

## THE INVENTION

Appellant's disclosed and claimed invention is directed to packet telephony devices with encryption keys configured to enable authentication, for increasing the security of online account access and transactions.

(Abstract.)

Claim 1, reproduced below, is illustrative of the claimed subject matter:

1. A VoIP packet telephony device, comprising:
  - a signaling module configured for receiving, processing, and generating VoIP telephony signaling packets;
  - a media module interconnected with said signaling module and configured for receiving, processing, and generating VoIP telephony media packets;
  - an encryption module interconnected with said signaling and media modules and having an encryption key encoded therein; and
  - a user actuable authentication trigger, wherein said VoIP packet telephony device is configured to transmit an authentication communication generated in part from said encryption key upon actuation thereof.

## REJECTIONS

The Examiner rejected claims 1–8 under 35 U.S.C. § 103(a) as being unpatentable over Mizrah (US 2008/0098464 A1, pub. Apr. 24, 2008) and Ikeda et al. (US 7,251,485 B2, issued July 31, 2007). (Final Act. 2–8.)

The Examiner rejected claims 9–16 under 35 U.S.C. § 103(a) as being unpatentable over Mizrah, Ikeda and Toennis et al. (US 7,965,701 B1, issued June 21, 2011). (Final Act. 8–18.)

## ISSUES ON APPEAL

Appellant’s arguments in the Appeal Brief present the following dispositive issues:<sup>2</sup>

Whether the Examiner erred in finding the combination of Mizrah and Ikeda teaches or suggests the “signaling module,” “encryption module,” “authentication trigger,” or “second interface” limitations recited in one or both of independent claims 1 and 5, and whether the Examiner erred in finding the combination of Mizrah, Ikeda and Toennis teaches or suggests the “signaling module” and “authentication interface” limitations recited in independent claim 9. (App. Br. 5–7, 13–14.)

## ANALYSIS

For the limitations of claims 1 and 5 at issue, and for the “signaling module” limitation of claim 9, the Examiner solely relies on the disclosure in Mizrah of a two-channel challenge-response authentication method using a mobile phone displaying a one-time authentication challenge message sent via SMS. (Final Act. 3, 6; Ans. 17–18; Mizrah Figs. 5, 7, 24, ¶¶ 98, 128, 142.) Appellant argues the cited figures and accompanying description in Mizrah do not teach or suggest the claim limitations at issue, in that the disclosure of a one-time challenge, and a general disclosure of the use of encryption, does not: (i) disclose a signaling module configured for “receiving, processing, and generating VoIP telephony signaling packets”

---

<sup>2</sup> Rather than reiterate the arguments of Appellant and the findings of the Examiner, we refer to the Appeal Brief (filed Feb. 23, 2015); the Reply Brief (filed Aug. 17, 2015); the Final Office Action (mailed Sep. 16, 2014); and the Examiner’s Answer (mailed June 15, 2015) for the respective details.

(for claims 1 and 5, and similarly for claim 9), (ii) provide any of the features of the claimed encryption module, such as having an encoded encryption key within (for claims 1 and 5), (iii) disclose an authentication trigger configured to transmit an authentication communication (for claim 1), or (iv) include a second interface for connection to a non-packet telephone (for claim 5). (App. Br. 6–10.)

At least for the “authentication trigger” limitation of claim 1 and the “second interface” limitation of claim 5, we agree with Appellant that the Examiner does not provide *prima facie* support for the rejections. “[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.” *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). The Examiner admits “Mizrah et al. does not specifically call out . . . an Authentication trigger. . . .” (Ans. 18.) The Examiner’s rationale for rejection is:

[T]he telephone is [a] standard phone that to one of ordinary skill in the art at the time of the invention was made, sends/receives packets (signals). Mizrah et al. discloses “conventional security methods preventing credential entropy leakage, like: ... data encryption while in transit” (0098).

(*Id.*) We are persuaded this is inadequate support for the rejections. Nor are the Examiner’s findings in the Final Action sufficiently informative. (Final Act. 3, 6.) For example, the Examiner finds no basis for a teaching or suggestion of a VoIP packet telephony device configured to “transmit an authentication communication generated in part from said encryption key,” or of an interface “adapted for connection to a non-packet telephone.” (App. Br. 9–10; Final Act. 3, 6.)

For the “authentication interface” limitation of claim 9, the Examiner relies on the disclosure in Toennis of an IP telephone connection server that provides secure communications. (Final Act. 10–11.) However, we agree with Appellant that there is no teaching or suggestion in the cited combination of the required interconnection between the authentication interface and the claimed “authentication module,” because, as discussed above, the Examiner provides no basis for a teaching or suggestion of the required “transmit[ing] an authentication communication generated in part from said encryption key.” (App. Br. 13–14.)

Therefore, on the record before us, we are constrained to find the Examiner errs in rejecting independent claims 1, 5, and 9.

#### CONCLUSIONS

For the reasons stated above, we do not sustain the obviousness rejections of independent claims 1 and 5 over Mizrah and Ikeda, and of independent claim 9 over Mizrah, Ikeda and Toennis. We also do not sustain the obviousness rejections of claims 2–4 and 6–8 over Mizrah and Ikeda, and of claims 10–16 over Mizrah, Ikeda and Toennis, which claims are dependent from claims 1, 5, or 9.

#### DECISION

We reverse the Examiner’s rejections of claims 1–16.

REVERSED