



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.
12/563,421	09/21/2009	Christian Aabye	79900-758391	6368
66945	7590	09/30/2019	EXAMINER	
KILPATRICK TOWNSEND & STOCKTON LLP/VISA			WINTER, JOHN M	
Mailstop: IP Docketing - 22				
1100 Peachtree Street			ART UNIT	
Suite 2800			PAPER NUMBER	
Atlanta, GA 30309			3685	
			NOTIFICATION DATE	
			DELIVERY MODE	
			09/30/2019	
			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):

KTSDocketing2@kilpatrick.foundationip.com
ipefiling@kilpatricktownsend.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CHRISTIAN AABYE, HAO NGO,
DAVID WILLIAM WILSON, GUSTAVO MARIATH ZEIDEN,
CHRIS PITCHFORD, and KIUSHAN PIRZADEH

Appeal 2018-001119
Application 12/563,421¹
Technology Center 3600

Before BARBARA A. BENOIT, JOHN D. HAMANN, and
JOYCE CRAIG, *Administrative Patent Judges*.

HAMANN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants file this appeal under 35 U.S.C. § 134(a) from the Examiner's non-final rejection of claims 1, 2, 4, 10–12, 15, 17–19, and 27–38. We have jurisdiction under 35 U.S.C. §§ 6 and 134 because Appellants' claims for a patent have been twice rejected. *Ex parte Lemoine*, Appeal No. 94-0216, at 9–10 (BPAI Dec. 27, 1994) (precedential in part).

We reverse.

¹ According to Appellants, the real party in interest is Visa International Service Association. App. Br. 2.

THE CLAIMED INVENTION

Appellants' claimed invention relates to processing payment transactions that are conducted using a mobile device, including updating transaction data stored on the mobile device via a cellular network. Spec.²

¶ 22. Claim 1 is illustrative of the subject matter of the appeal and is reproduced below.

1. A mobile device for use in conducting a payment transaction, comprising:

a processor;

a computer readable memory; and

a set of instructions stored in the computer readable memory, which when executed by the processor implement a method comprising:

conducting the payment transaction by communicating with a point of sale terminal over a first communication channel using a contactless element in the mobile device, and adjusting an accumulator stored in the mobile device by an initial transaction amount of the payment transaction;

receiving an encryption key to be used for encrypting and decrypting transaction data over a second communication channel from a mobile gateway associated with an encryption key server in response to conducting the payment transaction, the encryption key being generated by the encryption key server based on a request associated with the payment transaction, the second communication channel being different than the first communication channel, and the second communication channel utilizing a cellular communications network;

² Our Decision relies upon Appellants' Appeal Brief ("App. Br.," filed May 1, 2017), Reply Brief ("Reply Br.," filed Nov. 13, 2017), and Specification ("Spec.," filed Sept. 21, 2009), as well as the Examiner's Answer ("Ans.," mailed Sept. 15, 2017) and the Non-Final Office Action ("Non-Final Act.," mailed Dec. 1, 2016).

receiving encrypted data related to the payment transaction in response to conducting the payment transaction, the encrypted data comprising an actual transaction amount at the mobile device through the second communication channel after communicating with the point of sale terminal, wherein the actual transaction amount of the payment transaction is determined by the point of sale terminal modifying the initial transaction amount of the payment transaction;

decrypting the encrypted data related to the payment transaction using the encryption key; and

updating the accumulator stored in the mobile device using the decrypted data related to the payment transaction, the decrypted data comprising the actual transaction amount of the payment transaction such that the accumulator is adjusted by the difference between the actual transaction amount of the payment transaction and the initial transaction amount of the payment transaction.

REJECTIONS ON APPEAL

(1) The Examiner rejected claims 1, 2, 4, 10, 11, 19, and 27–37 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Fisher (US 2007/0156436 A1; published July 5, 2007), Arthur (US 2008/0208762 A1; published Aug. 28, 2008), Silver (US 7,580,873 B1; issued Aug. 25, 2009), and Yang (US 2008/0118069 A1; published May 22, 2008). Non-Final Act. 4–14.

(2) The Examiner rejected claim 12 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Fisher, Arthur, Silver, Yang, and Fognies (US 2007/0243856 A1; published Oct. 18, 2007). Non-Final Act. 14.

(3) The Examiner rejected claims 15 and 18 under 35 U.S.C. § 103(a) as being unpatentable over the combination³ of Fisher, Arthur, Silver, Yang, and Li (US 2010/0057620 A1; published Mar. 4, 2010). Non-Final Act. 15.

(4) The Examiner rejected claims 17 and 38 under 35 U.S.C. § 103(a) as being unpatentable over the combination of Fisher, Arthur, Silver, Yang, and Drudis (US 2009/0016538 A1; published Jan. 15, 2009). Non-Final Act. 15–16.

ISSUE

The dispositive issue for this appeal is whether the combination of Fisher, Arthur, Silver, and Yang teaches or suggests receiving an encryption key for encrypting and decrypting transaction data over a cellular communication channel.

ANALYSIS

We have reviewed the Examiner’s rejections in light of Appellants’ arguments that the Examiner errs. We find Appellants’ arguments discussed herein⁴ persuasive.

Appellants argue that the combination of Fisher, Arthur, Silver, and Yang fails to teach or suggest “receiving an encryption key to be used for

³ In rejecting claims 15 and 18, which depend from independent claim 10, the Examiner relied on claim 10’s rejection, but omitted listing some of the references from claim 10’s rejection. Non-Final Act. 15. We treat this as a harmless, typographical error.

⁴ Because we agree with at least one of the dispositive arguments advanced by Appellants, we need not reach the merits of Appellants’ other arguments.

encrypting and decrypting transaction data over a second communication channel . . . [which uses] a cellular communications network,” as recited in independent claims 1 and 10. App. Br. 11–12; Reply Br. 3–4. In particular, Appellants first argue that “[a]t best, Yang describes a key for connecting to a first network access device 180 (e.g., an access point).” App. Br. 12 (citing Yang ¶¶ 23, 50–52, Fig. 1).

Second, Appellants argue that although Yang teaches using a cellular network (e.g., the SMS gateway) for transmitting a key to a first network device, Yang does not teach that the first network device uses the cellular network for transmitting transaction data. *Id.* Lastly, Appellants argue that “‘to be used for encrypting and decrypting transaction data over a second communication channel’ utilizing a ‘cellular communications network’ is not ‘a statement of intended use,’ since the functions of the ‘encryption key’ are positively recited later in the claim” (e.g., “decrypting the encrypted data related to the payment transaction using the encryption key”). Reply Br. 3; App. Br. 12 n.1.

The Examiner finds that “the scope of this claim element is merely ‘receiving an encryption key’ and that the intended usage of the key is beyond the scope of the claim and as such does not have patentable weight.” Ans. 3 (citation omitted). The Examiner finds that Yang teaches “receiving an encryption key” via Yang’s teaching that “a key management server send[s] a key via SMS transmission to a mobile device.” *Id.* (citing Yang ¶ 22); *see also* Non-Final Act. 6–7 (citing Yang Abstract, ¶¶ 19–20, 22) (finding Yang teaches receiving an encryption key).

We agree with Appellants that the Examiner errs. First, we agree with Appellants that Yang describes a key for connecting to an access point,

rather than an encryption key for encrypting or decrypting transaction data. *E.g.*, Yang ¶¶ 19–20. More specifically, Yang discloses that its key is used by an access point to authenticate a device trying to connect to it. *E.g.*, *id.* ¶¶ 4–5, 19. Yang makes no mention of encryption. *See generally* Yang. In contrast, the claimed “encryption key” is used to decrypt encrypted transaction data received by a mobile device. *See* App. Br. 22 (reciting claim 1); *see also* Spec. ¶ 56 (describing encryption protocols, such as the public key infrastructure protocols). Thus, the Examiner errs in finding that the cited portion of Yang discloses “receiving an encryption key.”

We also agree with Appellants that the Examiner errs in finding that Yang discloses using its key for encrypting or decrypting transaction data received over a cellular network. The cited portions of Yang only teach using a cellular network for providing the key to the first network device. Yang ¶ 23, Fig. 1. Once a device is connected, the cited portions of Yang do not teach using the key. *Id.* at Abstract, ¶¶ 19–20, 22.

Lastly, we agree with Appellants that the Examiner errs in finding that, other than “receiving an encryption key,” the disputed limitation is an intended use, which does not have patentable weight. To the contrary, “to be used for encrypting and decrypting transaction data over a second communication channel . . . [which uses] a cellular communications network” is a fundamental characteristic of the claimed invention and relates to claim 1’s other limitations. *See Vizio, Inc. v. Int’l Trade Comm’n*, 605 F.3d 1330, 1340 (Fed. Cir. 2010) (“[C]onclud[ing] that . . . ‘for decoding’ . . . is properly construed as a claim limitation, and not merely a statement of purpose or intended use for the invention, because ‘decoding’ is the essence or a fundamental characteristic of the claimed invention.”); *In re Jasinski*,

508 F. App'x 950, 952 (Fed. Cir. 2013) (finding claim language that provided criteria to analyze other limitations limiting, rather than an intended use); App. Br. 22 (claim 1 further reciting “receiving encrypted data . . . through the second communication channel” and “decrypting the encrypted data . . . using the encryption key”). Accordingly, we find that the Examiner errs in finding that the disputed limitation recites an intended use.

Accordingly, we do not sustain the Examiner's rejection of independent claims 1 and 10, as well as claims 2, 4, 11, 19, and 27–37, which depend from one of these independent claims. We also do not sustain the Examiner's rejections of claims 12, 15, 17, 18, and 38, as these claims depend from independent claim 10, and the additional cited references do not cure the above deficiencies.

DECISION

We reverse the Examiner's decision rejecting claims 1, 2, 4, 10–12, 15, 17–19, and 27–38.

REVERSED