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.
13/677,451	11/15/2012	Karl Norrman	0110-812	7057

120491 7590 03/01/2018

Leffler Intellectual Property Law, PLLC
2010 Corporate Ridge
Suite 700
McLean, VA 22102

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2444	

NOTIFICATION DATE	DELIVERY MODE
03/01/2018	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):

info@leffleriplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte KARL NORRMAN and MONICA WIFVESSON

Appeal 2017-009239
Application 13/677,451[1]
Technology Center 2400

Before TERRENCE W. McMILLIN, KARA L. SZPONDOWSKI, and SCOTT B. HOWARD, *Administrative Patent Judges*.

HOWARD, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant appeals under 35 U.S.C. § 134(a) from the Final Rejection of claims 1, 3–11, 13, and 15–23, which constitute all of the claims pending in this application. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

---

[1] Appellant is the Applicant, Telefonaktiebolaget LM Ericsson, which, according to the Appeal Brief is the real party in interest. App. Br. 2.

THE INVENTION

The disclosed and claimed invention is directed to "the handover of calls between cellular communication systems that support different security contexts" devices. Spec. 1.[2]

Claim 1, reproduced below with the relevant language emphasized, is illustrative of the claimed subject matter:

> 1. A method of operating a first node to generate a security context for a client in a cellular communication system, wherein the first node comprises processing circuitry, the method comprising:
>
> *the first node performing, as part of a handover in the cellular communication system:*
>
> *receiving at least one cryptographic key from a second node;*
>
> *receiving identities of security algorithms supported by the client from a third node; and*
>
> *using the at least one cryptographic key and the identities to generate the security context for the client,*
>
> *wherein the first node is a target packet switched node, the third node is a source packet switched node, and the second node is a source circuit switched node.*

App. Br., Claims App., 21.

REFERENCES

The prior art relied upon by the Examiner as evidence in rejecting the claims on appeal is:

---

[2] We refer to the Specification filed Nov. 15, 2012 ("Spec."); Final Office Action mailed June 23, 2016 ("Final Act."); Appeal Brief filed Dec. 13, 2016 ("App. Br."); Examiner's Answer mailed Apr. 17, 2017 ("Ans."); and the Reply Brief filed June 18, 2017 ("Reply Br.").

Blom et al. (hereafter "Blom")	US 8,094,817 B2	Jan. 10, 2012
Shaw	US 2013/0122871 A1	May 16, 2013
Fransen	US 8,954,739 B2	Feb. 10, 2015

REJECTIONS

Claims 1, 3–5, 7–11, 13, 15–17, and 19–23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fransen and Shaw. Final Act. 5.

Claims 6 and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Fransen, Shaw, and Blom. Final Act. 8–9.

ANALYSIS

We have reviewed the Examiner's rejection in light of Appellant's arguments that the Examiner erred. In reaching this decision, we have considered all evidence presented and all arguments made by Appellant. We are persuaded by Appellant's arguments regarding the pending claims.

The Examiner finds Fransen's SGSN (Serving GPRS Support Node) teaches the claimed first node, and Fransen's HLR/AuC (Home Location Register/Authentication Center) teaches the claimed second node. Ans. 2–3 (citing Fransen Figs. 1, 2B, 4A, col. 7, l. 58.–col. 8, l. 3). The Examiner further finds Fransen teaches the first node receiving at least one cryptographic key from the second node, and the first node receiving identities of security algorithms from the third node. Final Act. 5–6 (citing Fransen Fig. 4, col. 9, ll. 8–17, 36–55, col. 9, l. 63–col. 10, l. 7). The Examiner relies on Shaw's SGSN 676 to teach the claimed first node, Shaw's another SGSN to teach the claimed third node, and Shaw's MSC 708 (Mobile Switching Center Server) to teach the claimed second node. Final

Act. 6 (citing Shaw ¶¶ 53–55, 58–59). The Examiner finds Shaw teaches the performance of the steps "as part of a handover in the cellular communication system," as claimed. Final Act. 6 (citing Shaw ¶¶ 77, 81–85).

Appellant argues Shaw teaches merely that MSC can perform handover, but does not teach handover methodology such as that recited in claim 1. App. Br. 12; Reply Br. 4. Appellant further argues that Fransen does not teach interactions between circuit switched and packet switched technology and does not teach a target packet switched node (i.e., the claimed first node) receiving anything from a source circuit switched node (i.e., the claimed second node). App. Br. 13–14.

We are persuaded by Appellant's arguments as the Examiner has not identified sufficient evidence or provided sufficient explanation as to how the combination of Shaw's SGSN 676, another SGSN, and MSC 708, with mention of handover capabilities, with Fransen's attach request to the SGSN and retrieved authentication response, teaches

> *the first node (target packet switched node) performing, as part of a handover in the cellular communication system: receiving at least one cryptographic key from a second node (source circuit switched node); receiving identities of security algorithms* supported by the client *from a third node (source packet switched node)*; and using the at least one cryptographic key and the identities to generate the security context for the client,

as recited in in claim 1 (emphasis added).

The cited section of Shaw describes "an attach request is sent by mobile subscriber 612 to SGSN 676," and the SGSN 676 "queries another SGSN, to which mobile subscriber 612 was attached before," and using the information to "authenticate mobile subscriber 612 to SGSN 676 by HLR

674." Shaw ¶ 53. Shaw further describes the MSC 708 "performs a switching function for the network" and also performs "other functions, such as . . . handovers." Shaw ¶ 58. The cited section of Fransen describes the MSC/SGSN receiving an attach request and issuing an authentication to the HLR to return authentication information including keys to the MSC/SGSN to compare and switch to security mode. Fransen col. 9, ll. 8–36. In other words, Shaw teaches SGSN 676 communicating with another SGSN to authenticate the mobile subscriber as well as the use of an MSC that can perform handover, and Fransen teaches MSC/SGSN communicating keys for authentication and security mode. However, Fransen and Shaw do not teach the limitations required by claim 1: that the target packet switched node (first node) performs, as part of a handover in the cellular communication system, receiving at least one cryptographic key from a source circuit switched node (second node); that the target packet switched node (first node) performs, as part of a handover in the cellular communication system, receiving identities of security algorithms supported by the client from a source packet switched node (third node); and that the target packet switched node (first node) performs, as part of a handover in the cellular communication system, using the at least one cryptographic key and the identities to generate the security context for the client.

Appellant further contends that Fransen and Shaw, even in combination, would merely result in "an authentication method in a communication system in which some other nodes perform handover," but this does not teach generating a security context as part of a handover from a circuit switched node to a packet switched node as required by claim 1. Reply Br. 4. The Examiner does not provide a reason to combine the teachings of Fransen and Shaw, or show that modifications would result in

performing handover by generating a security context from interactions between packet switched nodes and circuit switched nodes.

Therefore, we agree with Appellant that the Examiner's finding that the combination of Fransen and Shaw teaches the disputed limitation is in error because it is not supported by a preponderance of the evidence. *See In re Caveney*, 761 F.2d 671, 674 (Fed. Cir. 1985) (holding that the Examiner's burden of proving non-patentability is by a preponderance of the evidence); *see also In re Warner*, 379 F.2d 1011, 1017 (CCPA 1967) ("The Patent Office has the initial duty of supplying the factual basis for its rejection. It may not, because it may doubt that the invention is patentable, resort to speculation, unfounded assumptions or hindsight reconstruction to supply deficiencies in its factual basis.").

Accordingly, we are constrained on the record before us, to reverse the Examiner's § 103 rejection of claim 1, along with the § 103 rejection of claims 11, 13, and 23, which recite limitations commensurate in scope to the disputed limitation discussed above, and dependent claims 3–5, 7–10, 15–17, and 19–22. *See* App. Br. 17.

Moreover, because the Examiner has not shown that the additional references cure the foregoing deficiency regarding the rejection of the independent claims 1, 11, 13, and 23, we will not sustain the obviousness rejections of dependent claims 6 and 18. *See* App. Br. 17–19.

DECISION

For the above reasons, we reverse the Examiner's decisions rejecting claims 1, 3–11, 13, and 15–23.

REVERSED