

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NOKIA SOLUTIONS AND NETWORKS US LLC, and
NOKIA SOLUTIONS AND NETWORKS OY,
Petitioner,

v.

HUAWEI TECHNOLOGIES CO. LTD.,
Patent Owner.

Case IPR2017-00660
Patent 9,241,261 B2

Before JENNIFER MEYER CHAGNON,
MICHELLE N. WORMMEESTER, and CHRISTA P. ZADO,
Administrative Patent Judges.

CHAGNON, *Administrative Patent Judge.*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Nokia Solutions and Networks US LLC, and Nokia Solutions and Networks Oy (collectively, “Petitioner”)¹ filed a Petition for *inter partes* review of claims 1–5, 7–13, 15–21, 23, and 24 (“the challenged claims”) of U.S. Patent No. 9,241,261 B2 (Ex. 1001, “the ’261 patent”). Paper 1 (“Pet.”). Petitioner relies on the Declarations of David Lyon, Ph.D. (Ex. 1003) and Balazs Bertenyi (Ex. 1004) to support its positions. Huawei Technologies Co. Ltd. (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”).

We have authority to determine whether to institute *inter partes* review. *See* 35 U.S.C. § 314(b); 37 C.F.R. § 42.4(a). Upon consideration of the Petition and the Preliminary Response, and for the reasons explained below, we determine that the information presented shows a reasonable likelihood that Petitioner would prevail with respect to all of the challenged claims. *See* 35 U.S.C. § 314(a). Accordingly, we institute trial as to claims 1–5, 7–13, 15–21, 23, and 24 of the ’261 patent.

A. *Related Proceedings*

The parties indicate that the ’261 patent is the subject of the following ongoing district court proceeding: *Huawei Techs. Co. v. T-Mobile US, Inc.*, Case No. 2:16-cv-00057 (E.D. Tex.). Pet. 1; Paper 6, 2.

B. *The ’261 Patent*

The ’261 patent is titled “Method, System and Device for Negotiating Security Capability When Terminal Moves,” and was filed as

¹ Petitioner identifies T-Mobile USA, Inc. and T-Mobile US, Inc. as additional real parties-in-interest. Pet. 1.

U.S. application No. 14/303,146 on June 12, 2014. Ex. 1001, at [21], [22], [54]. The '261 patent claims priority, via a chain of continuation applications, to application PCT/CN2008/072165, filed on August 27, 2008. *Id.* at [63]. The '261 patent also claims priority to two Chinese applications: CN 2007 1 0145703, filed August 31, 2007, and CN 2007 1 0151700, filed September 26, 2007. *Id.* at [30].

The '261 patent “relates to the field of wireless communication technology, and more particularly to a method and a system for negotiating a security capability when a terminal moves, a mobility management entity (MME), and a user equipment (UE).” *Id.* at 1:18–22. Specifically, the '261 patent describes a method and system by which “a UE in an idle state can negotiate a security capability” “when moving from a 2G/3G network to an LTE network.” *Id.* at 2:14–20.

Figure 1 of the '261 patent is reproduced below.

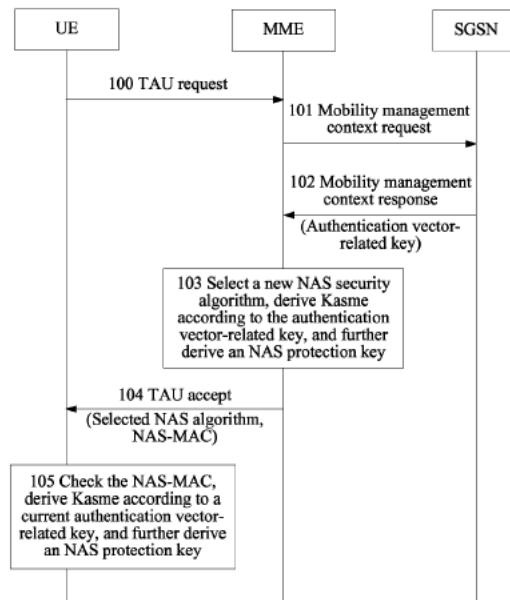


FIG. 1

Figure 1, reproduced above, is a flow chart of a method for negotiating a security capability when a terminal moves, according to an embodiment of the '261 patent. *Id.* at 4:3–5. According to the method illustrated in Figure 1, a UE sends a Tracking Area Update (TAU) request to an MME, at step 100. *Id.* at 4:47. The TAU request includes, among other things, the “security capability information supported by the UE,” which “includes an [non-access stratum (NAS)] security algorithm (an NAS integrity protection algorithm and/or an NAS confidentiality protection algorithm).” *Id.* at 4:54–64. At steps 101 and 102, “the MME acquires an NAS security algorithm supported by the UE, and sends a mobility management context request message to an SGSN. After receiving the message, the SGSN sends a mobility management context response message carrying an authentication vector-related key to the MME.” *Id.* at 4:65–5:3.

At step 103, “the MME selects a new NAS security algorithm, according to the NAS security algorithm supported by the UE and an NAS security algorithm supported by the MME as well as an NAS security algorithm allowed by the system.” *Id.* at 5:32–36. At step 104, “the MME generates a TAU accept message carrying the selected NAS security algorithm.” *Id.* at 5:41–42. At step 105, “the UE receives the TAU accept message carrying the NAS security algorithm selected by the MME, and acquires the negotiated NAS security algorithm.” *Id.* at 5:54–56. The UE then “derives a root key . . . according to a current authentication vector-related key . . . , and derives an NAS protection key according to the root key.” *Id.* at 5:57–63.

C. Illustrative Claims

Of the challenged claims, claims 1, 9, and 17 are independent. Claims 2–5, 7 and 8 depend from claim 1; claims 10–13, 15, and 16 depend from claim 9; claims 18–21, 23 and 24 depend from claim 17. Independent claims 1, 9, and 17 of the '261 patent are reproduced below, and are illustrative of the challenged claims. For convenience of the discussion, the claims are annotated with Petitioner's labeling of the claim elements.

1. [*I Pre*] A method of security negotiation for idle state mobility from a first network to a long term evolution (LTE) network using a mobility management entity (MME), the method comprising:

[*IA*] transmitting an authentication vector-related key from a service general packet radio service (GPRS) support node (SGSN) in the first network to the MME;

[*IB*] receiving security capabilities of a user equipment (UE) including non-access stratum (NAS) security capabilities of the UE from the UE;

[*IC*] selecting a NAS security algorithm supported by the NAS security capabilities of the UE;

[*ID*] sending a message that indicates the selected NAS security algorithm to the UE; and

[*IE*] deriving a NAS protection key with the selected NAS security algorithm from the authentication vector-related key.

Ex. 1001, 11:54–12:2.

9. [*9 Pre*] A communications system comprising:

[*9A*] an acquisition module that receives from a user equipment (UE) security capabilities of the UE including non-access stratum (NAS) security capabilities of the UE;

[*9B*] a service general packet radio service (GPRS) support node (SGSN) in a first network that sends an authentication vector-related key to the acquisition module;

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.