Trials@uspto.gov
Tel: 571-272-7822

Paper 12
Entered: May 10, 2018

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INAUTH, INC.,
Petitioner,

v.

MSIGNIA, INC.,
Patent Owner.

Case IPR2018-00150
Patent 9,559,852 B2

Before TREVOR M. JEFFERSON, JAMES B. ARPIN, and GREGG I. ANDERSON, *Administrative Patent Judges.*

ARPIN, *Administrative Patent Judge*.

DECISION
Denying Institution of Inter Partes Review
35 U.S.C. § 314(a)

I. INTRODUCTION

A. Background

InAuth, Inc. ("Petitioner") filed a Petition requesting an *inter partes* review of claims 1–25 of U.S. Patent No. 9,559,852 B2 (Ex. 1001, "the '852 patent"). Paper 2 ("Pet."). mSIGNIA, Inc. ("Patent Owner") filed a Preliminary Response. Paper 9 ("Prelim. Resp."). Having considered the Petition, the Preliminary Response, and the evidence of record, and applying the standard set forth in 35 U.S.C. § 314(a), which requires that Petitioner demonstrate a reasonable likelihood that it would prevail with respect to at least one challenged claim; we *deny* institution of *inter partes* review of claims 1–25 of the '852 patent.

B. Related Matters

The parties indicate that the '852 patent is the subject of a civil action identified as *mSIGNIA, Inc. v. InAuth, Inc.*, 8:17-cv-01289 (C.D. Cal.), filed July 26, 2017. Pet. 71 (citing Ex. 1027); Paper 5, 1. Petitioner states that InAuth, Inc. is a wholly owned subsidiary of American Express Travel Related Services Company, Inc., the corporate parent of which is American Express Company. Pet. 70. Thus, Petitioner states that InAuth, Inc., the American Express Company, and American Express Travel Related Services Company, Inc. are real parties-in-interest. *Id.* at 70–71. Patent Owner states that mSIGNIA is the real party-in-interest. Paper 5, 1.

C. The '852 Patent

The '852 patent is entitled "Cryptographic Security Functions Based on Anticipated Changes in Dynamic Minutiae" and is directed to "methods and systems for dynamic key cryptography us[ing] a wide range of minutiae as key material including computer hardware, firmware, software, user secrets, and user biometrics rather than stor[ing] a random number as a cryptographic key on the computer." Ex. 1001, 3:7–11. The '852 patent claims priority to U.S. Provisional Patent Application No. 61/462,474, filed February 3, 2011. *Id.* at [60]. Although Petitioner does not concede that the '852 patent is entitled to that priority date, the applied references predate that date, so, for purposes of this Decision, we accept the provisional application's filing date as the earliest effective filing date of the '852 patent. *See* Pet. 6 n.2.

The '852 patent recognizes that, in known authentication methods using "computer fingerprints," "[a] typical computer identifier is computed and remains *static*; to ensure reliability the computer fingerprint typically uses computer minutiae (e.g., serial numbers) *that normally do not change*. Thus, current computer fingerprints typically use a relatively small set of static minutia which may be prone to spoofing." Ex. 1001, 2:51–56 (emphases added); *see* Prelim. Resp. 1. Known methods, however, "allegedly did not provide for the use of minutia that is subject to change because routine changes to the minutia, e.g., an upgrade to a component, would alter the fingerprint and cause false identification of a device as 'different' (a 'false negative')." Pet. 1–2 (citing Ex. 1001, 2:56–3:2). The Specification of the '852 patent system explains that the disclosed systems and methods permit use of minutia that is subject to change, such as location

or hardware, firmware, or software versions, in the authentication process. Pet. 2; Prelim. Resp. 2. In particular, these systems and methods use information regarding "anticipated changes" to the minutia to "deliver[] a tolerant, yet secure authentication with fewer false negatives." Pet. 2 (quoting Ex. 1001, 5:40–44).

Figures 2A and 2B of the '852 patent are reproduced below.

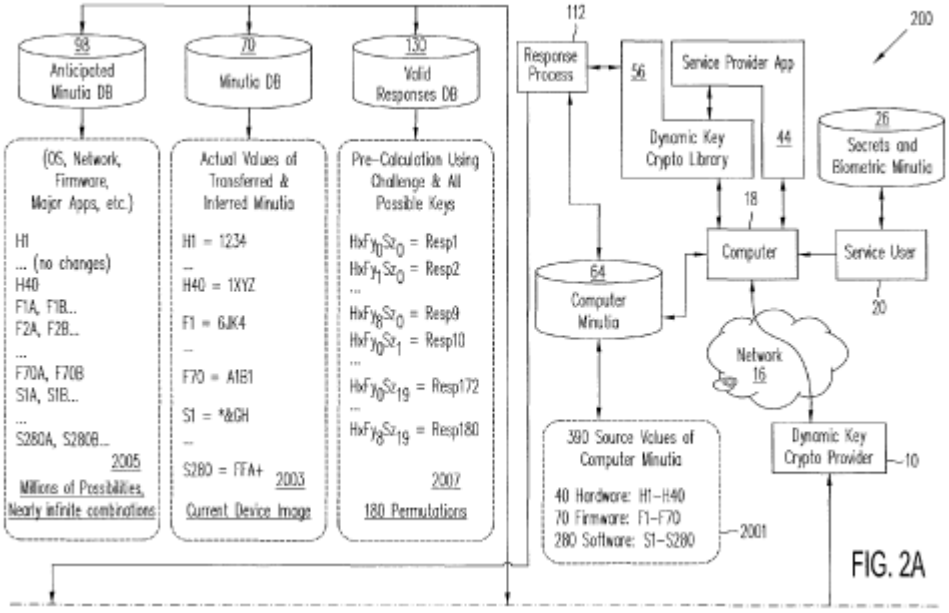

FIG. 2A

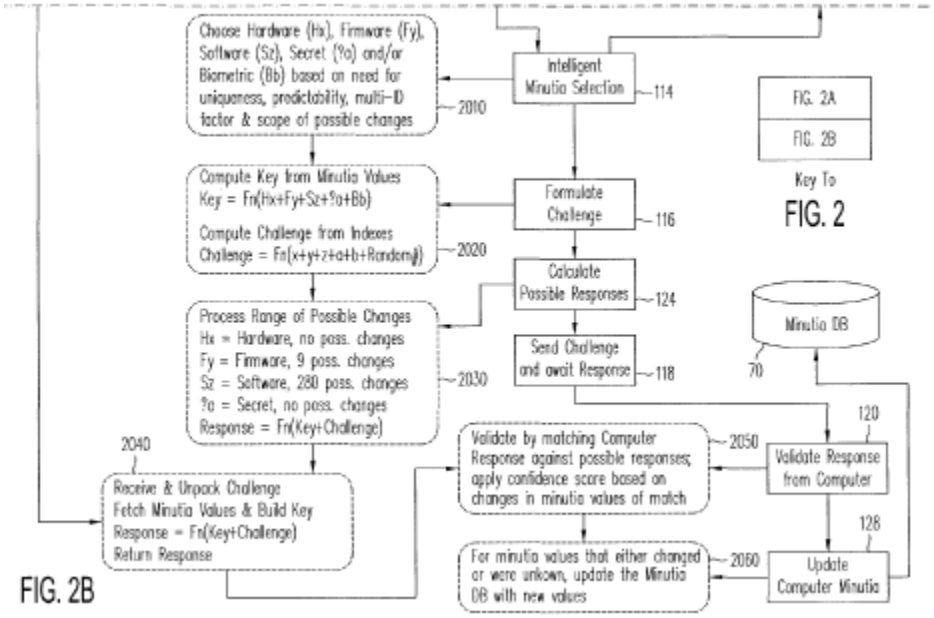

FIG. 2B

Figures 2A and 2B depict a system diagram illustrating a challenge, response and validation process performed by the system of Figure 1. Ex. 1001, 4:35–38.

More specifically, Figures 2A and 2B depict an example for providing and using dynamic key cryptography to ensure valid service user 20 is using authenticated computer 18 in system 200. *Id.* at 10:24–27. System 200 collects and catalogs minutiae values of computer 18 and service user 20 that may identify computer 18 and service user 20, such that computer minutia 64 and secrets and biometric minutia 26 may be used by dynamic key crypto provider 10 to form dynamic keys unique to each and every distinct computer 18 and service user 20. *Id.* at 10:27–34. Consequently, each distinct computer 18 may use unique computer minutia 64 and secrets and biometric minutia 26 in system 200 that correspond to that distinct computer 18 and service user 20, respectively, and "each uniquely identified computer 18 corresponds to one and only one distinct computer 18 and each uniquely identified service user 20 may correspond to one and only one

DOCKET ALARM

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.