(12) **United States Patent**
Miller et al.

(10) Patent No.: **US 8,817,984 B2**
(45) Date of Patent: **Aug. 26, 2014**

(54) **CRYPTOGRAPHIC SECURITY FUNCTIONS BASED ON ANTICIPATED CHANGES IN DYNAMIC MINUTIAE**

(75) Inventors: **Paul Timothy Miller**, Irvine, CA (US); **George Allen Tuvell**, Thompson's Station, TN (US)

(73) Assignee: **MSIGNIA, Inc.**, Irvine, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 187 days.

(21) Appl. No.: **13/366,197**

(22) Filed: **Feb. 3, 2012**

(65) **Prior Publication Data**

US 2012/0201381 A1 Aug. 9, 2012

Related U.S. Application Data

(60) Provisional application No. 61/462,474, filed on Feb. 3, 2011.

(51) **Int. Cl.**
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC **H04L 63/0876** (2013.01)
USPC **380/255**

(58) **Field of Classification Search**
CPC H04L 63/0876
USPC 380/255
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,185,316	B1 *	2/2001	Buffam	.... 382/115
7,330,871	B2	2/2008	Barber	
7,373,669	B2	5/2008	Eisen	
7,908,662	B2	3/2011	Richardson	
7,937,467	B2	5/2011	Barber	
2007/0124801	A1	5/2007	Thomas et al.	
2007/0174206	A1 *	7/2007	Colella	.... 705/64
2007/0214151	A1	9/2007	Thomas et al.	
2008/0244744	A1	10/2008	Thomas et al.	
2009/0138975	A1	5/2009	Richardson	
2010/0027834	A1 *	2/2010	Spitzig et al.	.... 382/100
2010/0229224	A1	9/2010	Etchegoyen	
2011/0082768	A1	4/2011	Eisen	
2011/0113388	A1	5/2011	Eisen et al.	
2011/0293094	A1	12/2011	Os et al.	
2011/0296170	A1	12/2011	Chen	

FOREIGN PATENT DOCUMENTS

WO   WO 2010/035202   4/2010

* cited by examiner

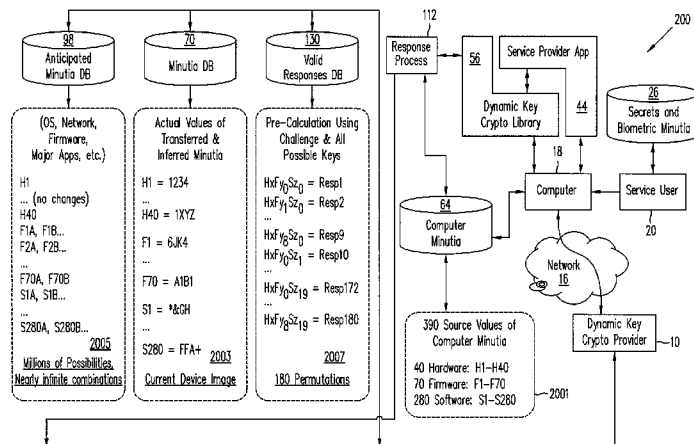*Primary Examiner* — Pramila Parthasarathy
Assistant Examiner — Dao Ho
(74) *Attorney, Agent, or Firm* — Haynes and Boone, LLP

(57) **ABSTRACT**

Dynamic key cryptography validates mobile device users to cloud services by uniquely identifying the user's electronic device using a very wide range of hardware, firmware, and software minutiae, user secrets, and user biometric values found in or collected by the device. Processes for uniquely identifying and validating the device include: selecting a sub-set of minutia from a plurality of minutia types; computing a challenge from which the user device can form a response based on the selected combination of minutia; computing a set of pre-processed responses that covers a range of all actual responses possible to be received from the device if the combination of the particular device with the device's collected actual values of minutia is valid; receiving an actual response to the challenge from the device; determining whether the actual response matches any of the pre-processed responses; and providing validation, enabling authentication, data protection, and digital signatures.
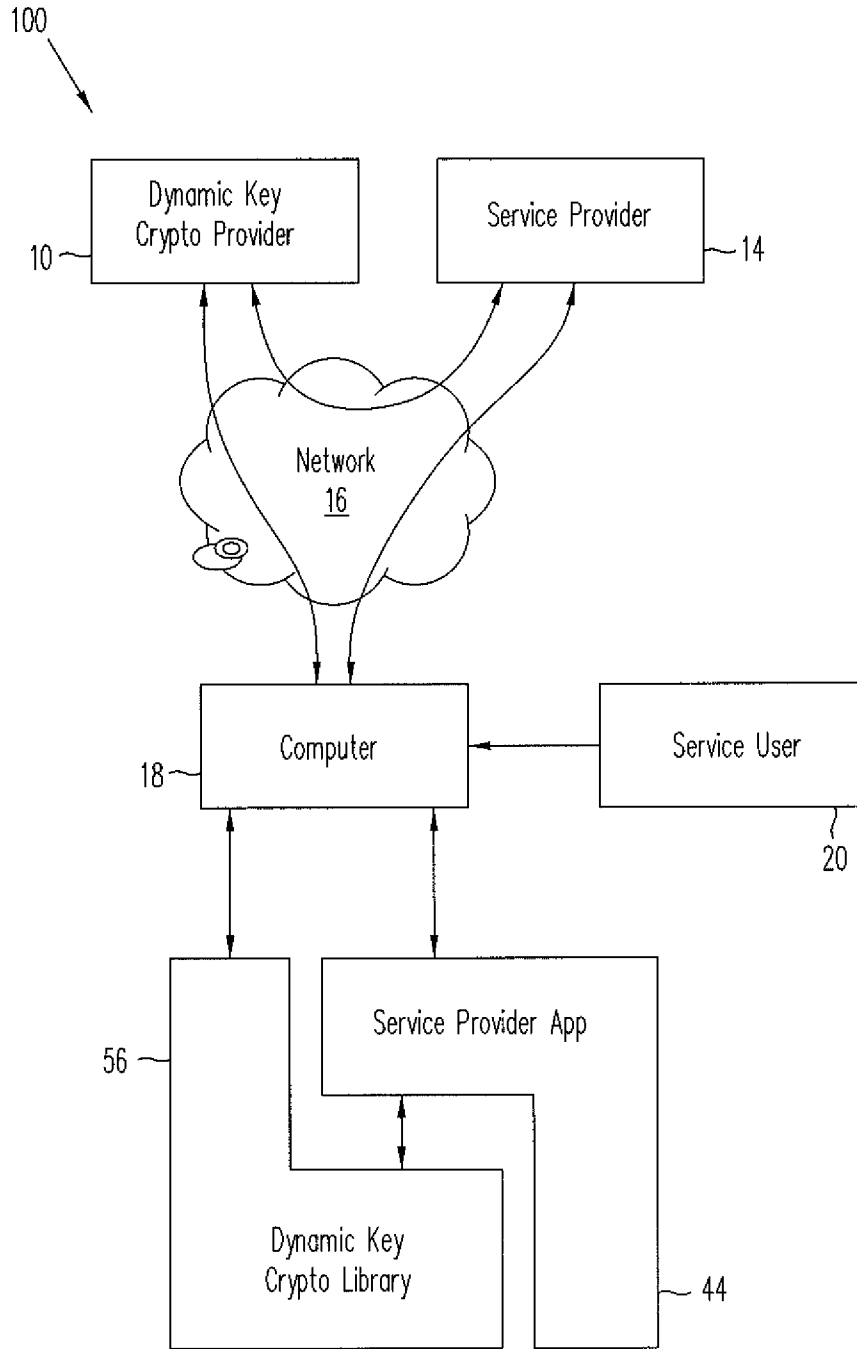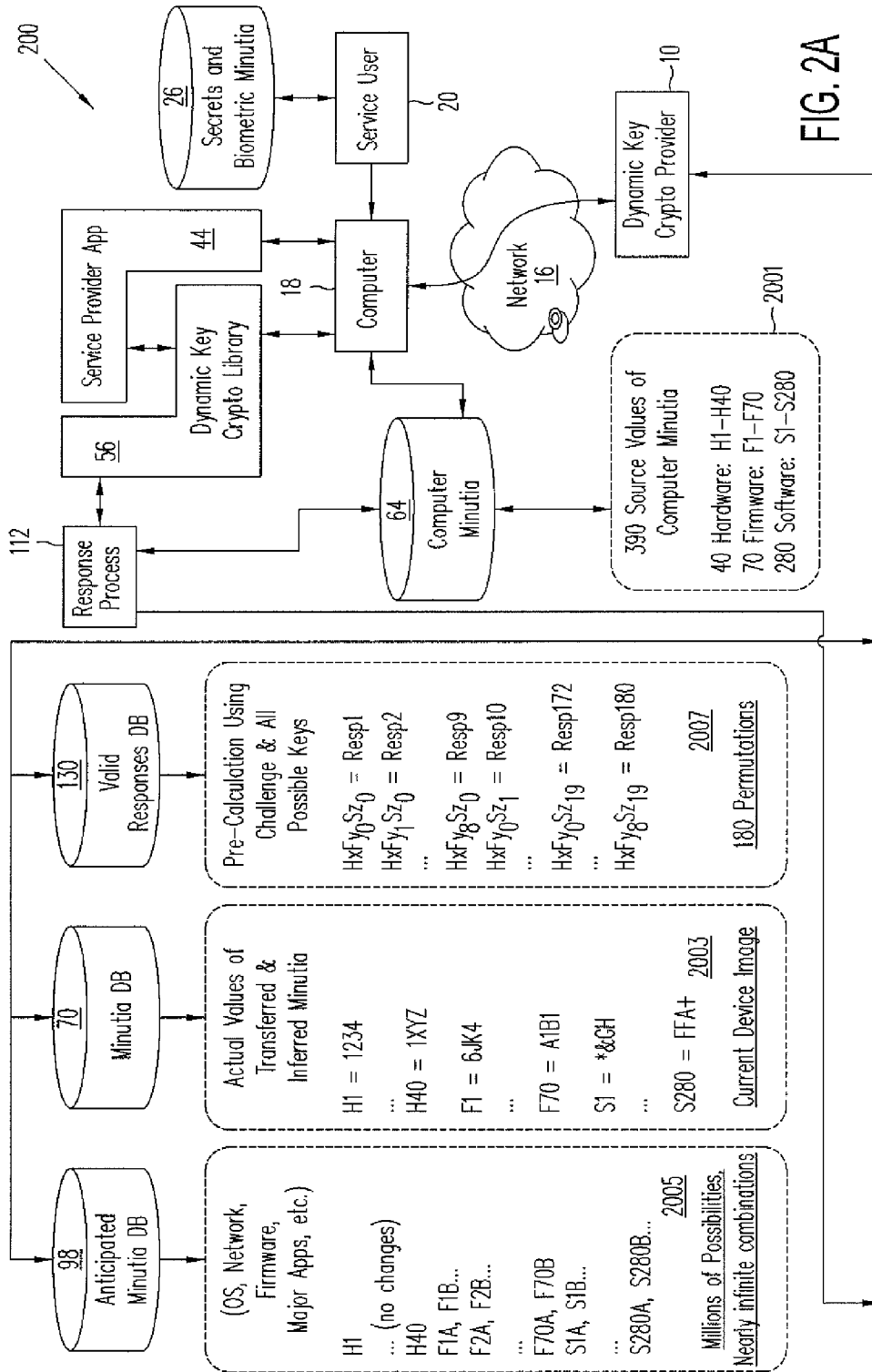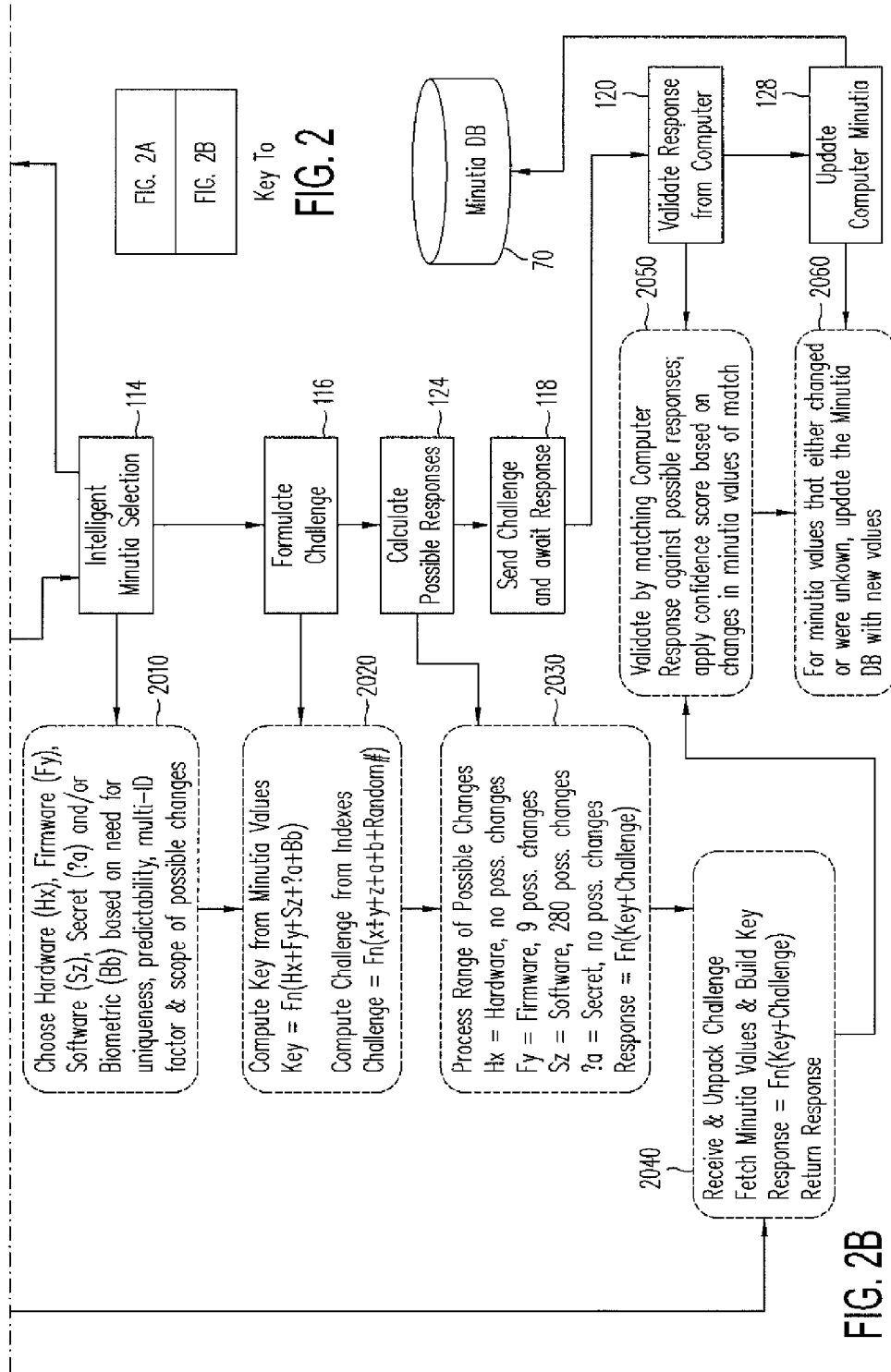
19 Claims, 11 Drawing Sheets

100

FIG. 1

FIG. 2A

Key To
FIG. 2

FIG. 2A
FIG. 2B

Minutia DB — 70

114 — Intelligent Minutia Selection

116 — Formulate Challenge

124 — Calculate Possible Responses

118 — Send Challenge and await Response

120 — Validate Response from Computer

128 — Update Computer Minutia

2010 — Choose Hardware (Hx), Firmware (Fy), Software (Sz), Secret (?a) and/or Biometric (Bb) based on need for uniqueness, predictability, multi-ID factor & scope of possible changes

2020 — Compute Key from Minutia Values
Key = Fn(Hx+Fy+Sz+?a+Bb)
Compute Challenge from Indexes
Challenge = Fn(x+y+z+a+b+Random#)

2030 — Process Range of Possible Changes
Hx = Hardware, no poss. changes
Fy = Firmware, 9 poss. changes
Sz = Software, 280 poss. changes
?a = Secret, no poss. changes
Response = Fn(Key+Challenge)

2040 — Receive & Unpack Challenge
Fetch Minutia Values & Build Key
Response = Fn(Key+Challenge)
Return Response

2050 — Validate by matching Computer Response against possible responses; apply confidence score based on changes in minutia values of match

2060 — For minutia values that either changed or were unkown, update the Minutia DB with new values

FIG. 2B

FIG. 3

DOCKET ALARM
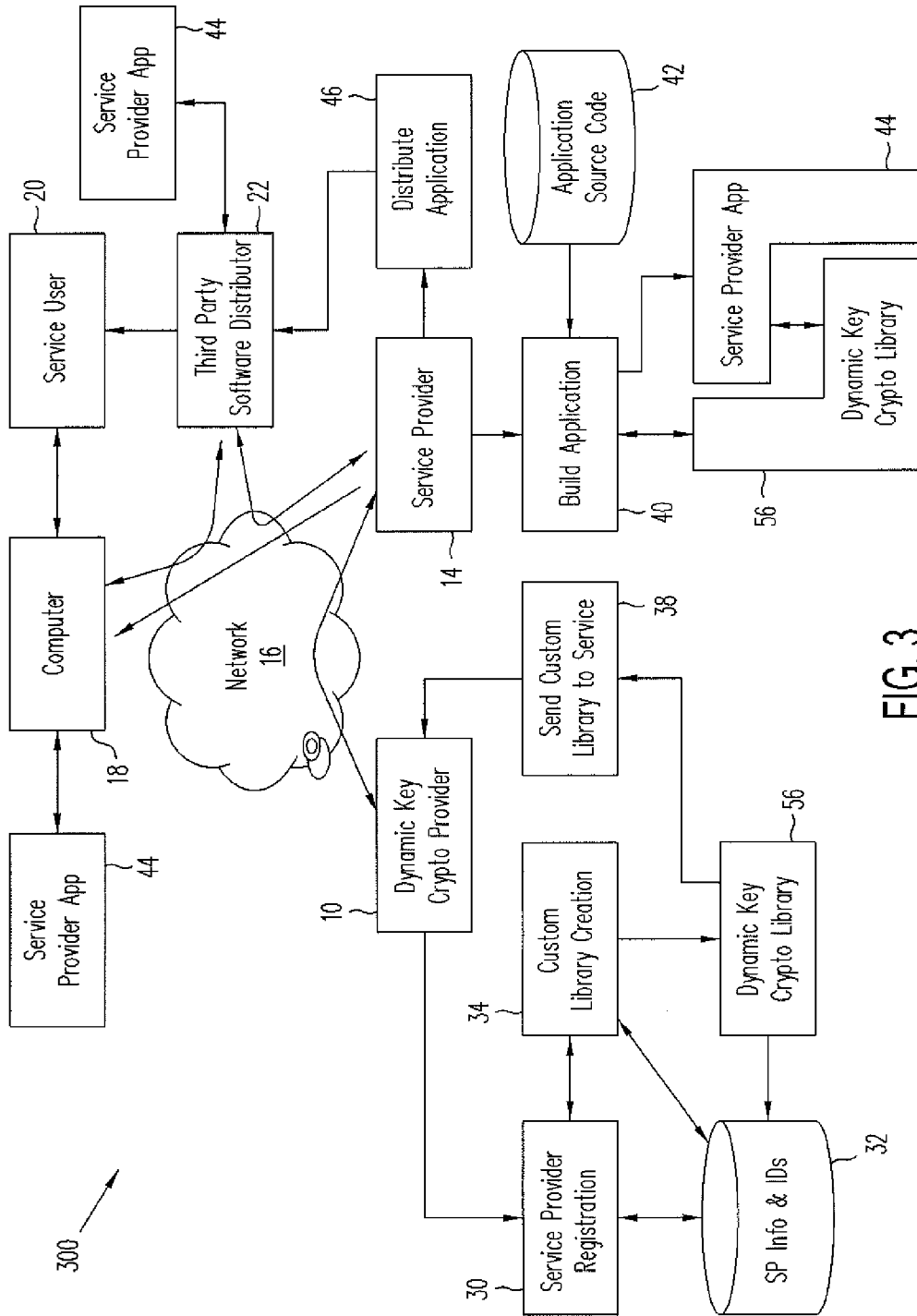
Explore Litigation Insights

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.