

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.

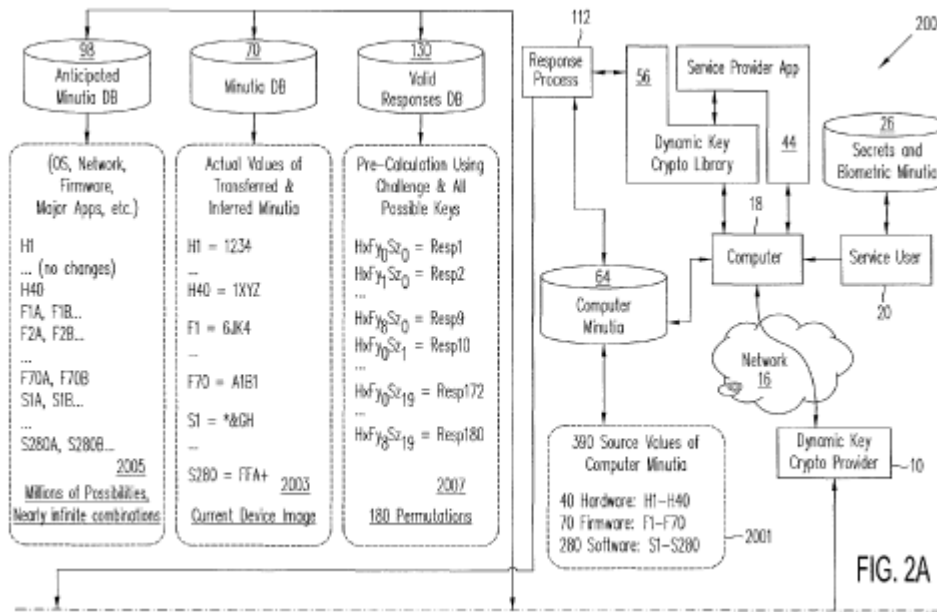
C. The '852 Patent

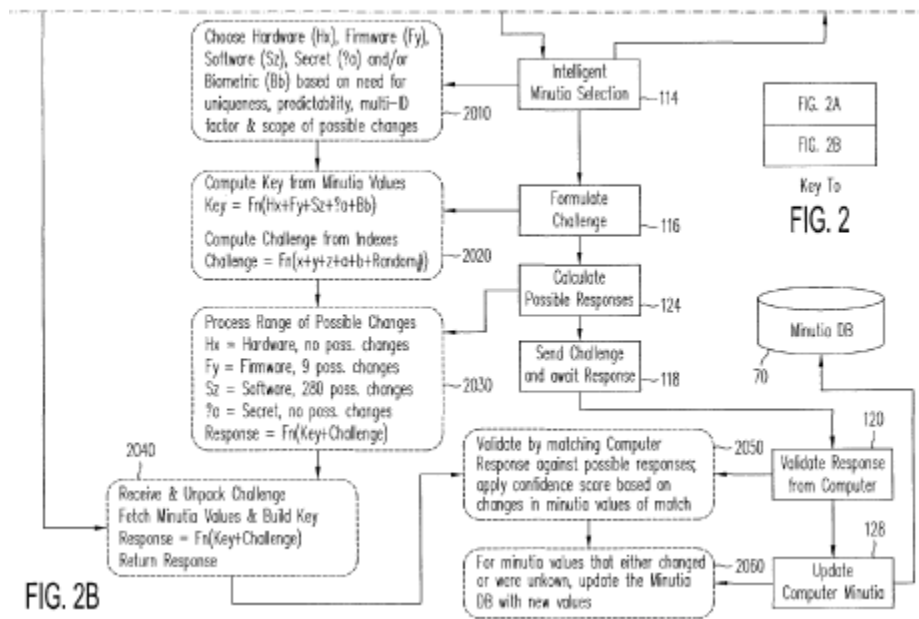
The '852 patent is entitled “Cryptographic Security Functions Based on Anticipated Changes in Dynamic Minutiae” and is directed to “methods and systems for dynamic key cryptography us[ing] a wide range of minutiae as key material including computer hardware, firmware, software, user secrets, and user 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.





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

distinct service user 20.” *Id.* at 10:34–41. “The unique identification of a computer 18 may be processed by system [200], for example, by a service provider 14 or by the dynamic key crypto provider 10, and there [may] be no meaningful single identifier or identity key itself stored on the computer 18.” *Id.* at 10:42–46.

System 200 depicts a system for identifying and authenticating a specific computer 18 and service user 20 via challenge, response, and validation sequences performed by dynamic key crypto provider 10. *Id.* at 10:46–50. Each distinct computer 18 and service user 20 is recognized by specific computer minutia 64, specific secrets and biometric minutia 26, or combinations thereof found on computer 18 or collected by computer 18 from service user 20 as cataloged by dynamic key crypto provider 10. *See id.* at 10:50–58.

As shown in Figure 2A, at step 2001, “computer minutia 64 can represent a set of 390 distinct minutiae values that may be chosen for collecting and cataloging from the computer 18.” *Id.* at 11:22–24. For example, hardware minutia (Hx) may represent 40 categories or types of the minutia, firmware minutia (Fx) may represent 70 categories or types of the minutia, software minutia (Sx) may represent 280 categories or types of the minutia, service user 20 secrets (?x) may represent 2 specific secrets, and service user 20 biometric minutia (Bx) may represent 5 categories or types of the minutia, from which it may be possible to accurately and uniquely identify specific computer 18 and associated service user 20 for computer 18. *Id.* at 11:21–28, 12:37–49. “Hardware minutia values typically cannot change without changing a physical component of the computer 18. Firmware minutia can be updated but usually their update is controlled by

someone other than the service user 20. Software minutia changes dynamically via various individual instantiations of service user 20 and includes elements that may require predictable, constant change in normal situations (i.e., frequently called contact phone numbers).” *Id.* at 11:38–46. Software minutiae values, however, may reflect customizations performed by service user 20. Thus, “software minutiae values can accurately identify computer 18 devices that are otherwise extremely similar in hardware and firmware.” *Id.* at 11:49–51.

Referring to Figure 2B, at step 2020, formulate challenge 116 process computes a cryptographic key based on a combination of minutia (e.g., Hx-Fy-Sz for the illustrated example). *Id.* at 15:43–46. At step 2030, dynamic key crypto provider 10 computes all responses that are acceptable from computer 10. *Id.* at 16:8–10.

At step 2040, the particular computer 18 being challenged may receive the challenge and unpack the challenge to determine which minutia it should collect and use the values of to form its response to the challenge. Having unpacked the challenge using information and algorithms stored in the dynamic key crypto library 56, the response process 112 can use the computer 18 to fetch the values of the selected computer minutia 64 or collect the values of selected service and biometrics minutia 26 and build a key that may be identical to the key computed by the dynamic key crypto provider 10 at step 2020.

...

As illustrated at step 2050, the validate response from computer 120 process can therefore be determined by simply comparing the actual response received from the computer 18 to the allowable responses that are pre-processed by the dynamic key crypto provider 10 to determine if there is a match. Decrypting or decoding of a response is not necessary so the validation can occur very quickly.

Id. at 16:42–52, 17:1–7.

D. Illustrative Claim

Claims 1, 24, and 25 are independent, and each is directed to an identity recognition system. *Id.* at 34:18–47 (claim 1), 36:6–38 (claim 24),¹ 36:39–37:7 (claim 25). Each of claims 2–23 depends directly or indirectly from claim 1. *Id.* at 34:48–36:5. Claim 1 is illustrative and is reproduced below, with emphasis added.

1. A identity recognition system comprising:

a non-transitory memory storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and *(b) information regarding anticipated changes to one or more of the stored data values associated with that identity;*

one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations comprising:

generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values associated with the identity;

receiving, from the computer, the response to the challenge;

determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values

¹ Claim 24 is corrected by a Certificate of Correction.

associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value; and

recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.

Id. at 34:18–47 (disputed limitations emphasized).

E. Applied References and Declaration

Petitioner relies on the following references and declaration in support of its asserted grounds for unpatentability.

Exhibit No.	Declaration or Reference
1003	Declaration of Patrick Traynor, Ph.D.
1004	U.S. Patent No. 8,316,421 B2 to Etchegoyen <i>et al.</i> , filed October 13, 2010; published April 21, 2011; and issued November 20, 2012 (“Etchegoyen”) ²
1005	U.S. Patent Publication No. 2006/0282660 A1 to Varghese <i>et al.</i> , filed April 28, 2006, and published December 14, 2006 (“Varghese”)
1006	U.S. Patent No. 8,312,157 B2 to Jakobsson <i>et al.</i> , filed July 16, 2009; published January 20, 2011; issued November 13, 2012 (“Jakobsson”)

Pet. iv, 9, 11.

F. Asserted Grounds of Unpatentability

Petitioner argues that claims 1–25 of the ’852 patent are unpatentable based on the following grounds:

Reference(s)	Basis	Claim(s)
Etchegoyen	35 U.S.C. § 102	1–5, 7, 14–21, 24, and 25

² Based on its claim of priority to U.S. Provisional Patent Application No. 61/252,960, filed October 19, 2009, Dr. Traynor argues that Etchegoyen is entitled to a priority date of October 19, 2009. Ex. 1003 ¶¶ 61–64.

Etchegoyen	35 U.S.C. § 103	1–5, 7, 14–21, 24, and 25
Etchegoyen and Jakobsson	35 U.S.C. § 103	6 and 8–12
Etchegoyen and Varghese	35 U.S.C. § 102	13, 22, and 23
Varghese	35 U.S.C. § 102	1–23 and 25
Varghese	35 U.S.C. § 103	24

Pet. 5.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, “[a] claim in an unexpired patent that will not expire before a final written decision is issued shall be given its broadest reasonable construction in light of the specification of the patent in which it appears.” 37 C.F.R. § 42.100(b). In determining the broadest reasonable construction, we presume that claim terms carry their ordinary and customary meaning. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). This presumption may be rebutted when a patentee, acting as a lexicographer, sets forth an alternate definition of a term in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

1. “generating a challenge” (Claims 1, 24, and 25)

Petitioner and Patent Owner agree that only the term: “generating a challenge” recited in each independent claim requires express construction. Pet. 13; Prelim. Resp. 4–5; see Paper 11. Moreover, Petitioner and Patent Owner agree that “generating a challenge” should be construed as “generating a request for information.” Pet. 13; Prelim. Resp. 4. Nevertheless, Patent Owner further clarifies that the “challenge” is a challenge to the computer that is to be authenticated. Prelim. Resp. 4. We

believe that this clarification is apparent from the context in which the construed term is used in the independent claims. *See* Pet. 13 (“As used in the specification, the challenge is a request to the computer to provide information based on selected minutia.”). On this record and for purposes of this Decision, we adopt the parties’ agreed upon construction, in view of Patent Owner’s clarification that the challenge is to the computer seeking authentication, as the broadest reasonable interpretation of this term.

2. Other Claim Terms

Only terms which are in controversy need to be construed, and then only to the extent necessary to resolve the controversy. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))). For purposes of this Decision, no other claim terms require express construction.

B. Asserted Grounds

1. Overview

Petitioner argues that claims 1–5, 7, 14–21, 24, and 25 of the ’852 patent are anticipated by or, in the alternative, rendered obvious over the teachings of Etchegoyen and relies upon the Declaration of Dr. Traynor (Ex. 1003) to support its arguments. Pet. 5, 14–38; *see supra* Section I.F. Further, Petitioner argues that each of claims 6, 8–13, 22, and 23 are rendered obvious over the teachings of Etchegoyen in combination with those of Jakobsson or Varghese, and again relies upon the Declaration of

Dr. Traynor (Ex. 1003) to support its arguments. Pet. 5, 38–47; *see supra* Section I.F. In addition, Petitioner argues that claims 1–25 of the ’852 patent are anticipated by or, in the alternative, rendered obvious over the teachings of Varghese and relies upon the Declaration of Dr. Traynor (Ex. 1003) to support its arguments. Pet. 5, 47–70; *see supra* Section I.F.

As noted above, each of claims 2–23 depends directly from independent claim 1, and Patent Owner focuses its opposition primarily to the asserted grounds for unpatentability on the application of the teachings of Etchegoyen or Varghese to claims 1, 24, and 25. Prelim. Resp. 11–20, 25–28.

After reviewing Petitioner’s and Patent Owner’s arguments and evidence, for the reasons set forth below, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that any of claims 1–25 of the ’852 patent is unpatentable with respect to the grounds based, in whole or in part, on Etchegoyen or Varghese. Consequently, we *deny* institution of *inter partes* review of claims 1–25 of the ’852 patent as to the asserted grounds.

2. *Legal Principles*

“A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *Verdegaal Bros. v. Union Oil Co.*, 814 F.2d 628, 631 (Fed. Cir. 1987). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test. *See In re Bond*, 910 F.2d 831, 832 (Fed. Cir. 1990). Moreover, “it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art

would reasonably be expected to draw therefrom.” *Application of Preda*, 401 F.2d 825, 826 (CCPA 1968). Nevertheless,

unless a reference discloses within the four corners of the document not only all of the limitations claimed *but also all of the limitations arranged or combined in the same way as recited in the claim*, it cannot be said to prove prior invention of the thing claimed, and thus, cannot anticipate under 35 U.S.C. § 102.

Net MoneyIN, Inc. v. VeriSign, Inc., 545 F.3d 1359, 1371 (Fed. Cir. 2008) (emphasis added); accord *In re Arkley*, 455 F.2d 586 (CCPA 1972).

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

Obviousness is a question of law, which is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art;³ and (4) when in evidence,

³ Petitioner proposes an assessment of the level of ordinary skill in the art. Pet. 12; see Ex. 1003 ¶¶ 22, 23. Petitioner’s declarant, Dr. Traynor, exceeds this assessed level. Ex. 1003 ¶¶ 9–20. At this time, Patent Owner does not propose an alternative assessment. For purposes of this Decision, and to the extent necessary, we adopt Petitioner’s assessment.

objective evidence of nonobviousness.⁴ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

3. *Asserted Anticipation by and/or Obviousness Over Etchegoyen*

Petitioner argues that claims 1–5, 7, 14–21, 24, and 25 are unpatentable under 35 U.S.C. §§ 102(e) or 102(a) as anticipated by Etchegoyen or under 35 U.S.C. § 103(a) as rendered obvious over Etchegoyen. Pet. 5, 14–38. Relying on the testimony of its declarant, Dr. Traynor, Petitioner explains how Etchegoyen allegedly discloses each and every element of the challenged claims. *Id.* (citing Ex. 1003). We begin our analysis with an overview of Etchegoyen.

a. *Etchegoyen (Ex. 1004)*

Etchegoyen is entitled “System and Method for Device Authentication with Built-in Tolerance” and describes systems performing the following computer-implementable steps:

- (a) receiving and storing a first digital fingerprint of the device *during a first boot* of an authenticating software on the device, the first digital fingerprint based on *a first set of device components*, (b) receiving a second digital fingerprint from the device at a subsequent time, (c) comparing the second digital fingerprint with a plurality of stored digital fingerprints of known devices, (d) *in response to the comparison indicating a mismatch between the second digital fingerprint and the plurality of stored digital fingerprints, generating a request code comprising instructions for the device to generate a third digital fingerprint using the first set of device components*, (e) sending the request code to the remote device, (f) receiving the third digital fingerprint from

⁴ Patent Owner does not present arguments or evidence of such secondary considerations in the Preliminary Response. See Pet. 70.

the remote device in response to the request code, and
(g) authenticating the device based on a comparison of the
first and third digital fingerprints.

Ex. 1004, [57] (emphases added). Specifically, Etchegoyen describes that:

The first boot fingerprint may be generated using the overall environmental information collected by the authentication module. Alternatively, the first boot fingerprint may be generated using specific components of the device as predetermined by the authentication client. The specific components may include components from a typical-upgrade components list or a non-typical-upgrade components list. The typical-upgrade components list may include components such as: graphic card, random access memory, sound card, network adaptor, hard drive, CD/DVD drive, Ethernet controller, or other routinely upgraded components. The non-typical-upgrade components list may include components such as: motherboard, USB host controller, central microprocessor, PCI Bus, System CMOS Clock, etc.

Id. at 4:63–5:9 (emphasis added).

Etchegoyen's Figure 4 is reproduced below.

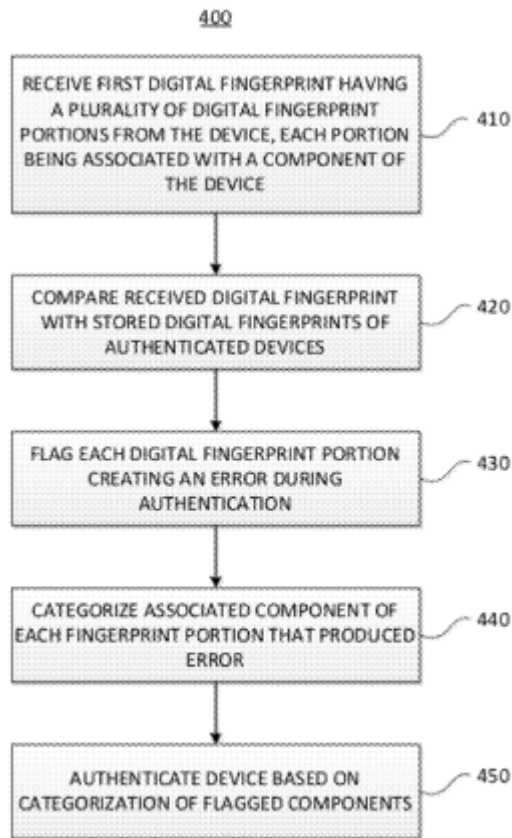


FIG. 4

Figure 4 is a process flow chart illustrating an embodiment of computer-implementable steps of a method for device authentication with built-in tolerance. *Id.* at 4:16–18; *see* Ex. 1003 ¶¶ 74–77.

Figure 4 depicts an exemplary process flow on the authenticating server side of method 400 for authenticating a device. Ex. 1004, 12:16–57. At step 410, a digital fingerprint is received by the authentication server. The digital fingerprint may have a plurality of digital fingerprint portions, and each portion represents a digital fingerprint of a component of the device. *Id.* at 12:21–23. For example, the digital fingerprint may include a plurality of mini-fingerprints, each associated with a different component of

the device, which may be combined to form the digital fingerprint. *Id.* at 12:23–27.

At step 420, the received digital fingerprint is authenticated by comparing it against stored digital fingerprints. *Id.* at 12:28–29. In particular, each portion of the received digital fingerprint may be compared with portions of a stored digital fingerprint. *Id.* at 12:29–31. If a portion of the received digital fingerprint matches any portion(s) of a stored digital fingerprint, a match of that portion is recognized. *Id.* at 12:31–34. If, however, the authenticating server fails to find a match for a portion of the received digital fingerprint, as indicated in step 430, that portion may be flagged as *failed*. *Id.* at 12:34–36. Alternatively, received digital fingerprint portions with matched portions in a stored digital fingerprint may be flagged as *passed*. *Id.* at 12:36–38.

In one embodiment, the device may be authenticated solely based on the ratio of passed and failed digital fingerprint portions. For example, if 80% of the portions are flagged as passed, then the device may be validly authenticated. *However, additional safeguards may be added to the authentication process by breaking down the components responsible for the errors.*

Id. at 39–45 (emphasis added); see *id.* at 13:22–38 (describing step 450). In step 440, each portion of the digital fingerprint may be *categorized* by its associated component. Ex. 1004, 12:45–46. By decoding the fingerprint portion, information about the component, such as the type of component used to generate the digital fingerprint portion, may be determined; and when the component information is analyzed, the component may be categorized as a typical-upgrade component or a non-typical-upgrade component. *Id.* at 12:49–55. “Thus, each fingerprint portion may be

compared against stored fingerprints, flagged as failed or passed, *and categorized.*” *Id.* at 12:55–57 (emphasis added).

b. Analysis With Respect to Independent Claims 1, 24, and 25

Petitioner argues that Etchegoyen discloses each and every element recited in independent claim 1. Pet. 14–23. Petitioner applies substantially the same mapping of Etchegoyen to independent claims 24 (*id.* at 23–26) and 25 (*id.* at 26–28). In the alternative, Petitioner argues that:

With respect to Claims 1, 24, and 25, to the extent Patent Owner contends that *Etchegoyen* does not anticipate because it does not disclose a single embodiment that uses both the request/response protocol (*i.e.*, challenge/response protocol) to obtain a fingerprint and the typical-upgrade ratio to analyze the fingerprint, it would have been obvious to a [person of ordinary skill in the art] to modify the embodiments disclosed to include both aspects.

Id. at 37 (citing Ex. 1003 ¶ 151). Patent Owner contends, however, that Etchegoyen fails to disclose the limitations of claim 1 relating to “anticipated changes” including “storing information associated with one or more identities, wherein the information stored for an identity includes (a) data values associated with that identity; and (b) *information regarding anticipated changes to one or more of the stored data values associated with that identity*” and “determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is *based on an acceptable change to a corresponding stored data value.*” Prelim. Resp. 7–11. For the reasons discussed below, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that

Etchegoyen discloses each and every element or teaches or suggests all of the limitations recited in independent claims 1, 24, and 25.

i. Petitioner's Mapping of Etchegoyen onto Claim 1

Petitioner provides a detailed mapping of the disclosure of Etchegoyen onto the elements of independent claim 1. Pet. 14–23; see Ex. 1003 ¶¶ 78–95. Specifically, Petitioner argues that Etchegoyen discloses a system for authenticating the identity of a device. Ex. 1004, 1:30–43. Similar to the system recited in claim 1, Etchegoyen's system recognizes that it is “desirable to provide an authentication method with built in flexibility or tolerance *to allow for some upgrades or changes to the device.*” *Id.* (emphasis added). Petitioner argues that Etchegoyen discloses “a non-transitory memory storing information associated with one or more identities” of the device to be authenticated. Pet. 18–19; see Ex. 1001, 34:19–21. Specifically, challenged claim 1 recites two types of stored information, namely, “(a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity.” Ex. 1001, 34:21–24. Petitioner argues that Etchegoyen's “first boot fingerprint” corresponds to the “data values” recited in claim 1. Pet. 15 (citing Ex. 1004, 4:56–62), 19. Further, Petitioner argues that Etchegoyen's “predetermined non-typical-upgrade component/typical-upgrade component ratio” and Etchegoyen's lists of typical-upgrade components and non-typical-upgrade components disclose the “information regarding anticipated changes to one or more of the stored data values.” *Id.* at 19–20 (citing Ex. 1004, 3:12–17, 4:65–5:2, 12:45–57, 13:22–38).

Claim 1 further recites “one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations.” Ex. 1001, 34:25–29. Petitioner argues that, referring to its Figure 1, Etchegoyen’s Processing Module 160 in communication with Storage Module 155 discloses this additional hardware. Pet. 16, 20 (citing Ex. 1004, 3:2–37, 9:49–52).

Claim 1 recites four method steps performed by the “one or more hardware processors.” Ex. 1001, 34:30–47. Petitioner argues that Etchegoyen discloses each of these steps. Specifically, claim 1 recites the step of “generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values associated with the identity.” *Id.* at 34:30–34. In view of the agreed construction of the term “generating a challenge” (*see supra* Section II.A.1.), Petitioner argues that Etchegoyen discloses “generat[ing] a request code,” which corresponds to generating the recited challenge. Pet. 20 (citing Ex. 1004, 5:35–39). Petitioner argues that Etchegoyen’s request code prompts the challenged computer to “send a response that includes a fingerprint or mini-fingerprint, such as a fingerprint based on the same components used for the first boot fingerprint.” *Id.* at 20 (citing Ex. 1004, 11:13–22); *see* Ex. 1004, 5:47–51.

Claim 1 further recites the step of “receiving, from the computer, the response to the challenge.” Ex. 1001, 34:35–36. Petitioner argues that Etchegoyen discloses that the recited “response to the challenge” in the form

of a “response code” that is generated in response to the request code is transmitted to the authenticating server. Pet. 21 (citing Ex. 1004, 5:44–63).

Claim 1 further recites “determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value.” Ex. 1001, 34:37–43. Referring to steps 420–450 of Etchegoyen’s Figure 4, discussed above, Petitioner argues that:

At step **420**, the system “compar[es] each portion of the received digital fingerprint with portions of a stored digital fingerprint.” [Ex. 1004], 12:28-29. At step **430**, the system “flag[s] each digital fingerprint portion creating an error during authentication.” *Id.*, 3:10-12. At step **440**, the system “categorize[s] associated component[s] of each fingerprint portion that produced the error.” *Id.*, 3:12-14. As discussed above, this step entails categorizing the flagged portions as corresponding to “typical-upgrade components” or “non-typical-upgrade components.” *And lastly at step 450, the system “authenticate[s] device based on categorization of flagged components.” Id.*, 15:42-43.

The determining step of *Etchegoyen* “us[es] the stored information regarding anticipated changes to the stored data values associated with the identity” both because it uses the predetermined typical-upgrade ratio and because it uses information regarding whether a failed mini-fingerprint corresponds to a “typical” or “non-typical” upgrade component.

The determining step of *Etchegoyen* also includes “determin[ing] whether a data value used to form the response is based on an acceptable change to a corresponding stored data value.” *Etchegoyen* discloses that one way of determining whether the response is based on an acceptable change to the stored data value (fingerprint) is evaluate whether the response has an acceptable typical-upgrade ratio (*e.g.*, less than one). *Id.*,

13:34-38. If the fingerprint changes in such a way that it still satisfies the requisite typical-upgrade ratio, the received fingerprint is based on an acceptable change to the stored data value (a previously stored fingerprint).

Pet. 21–22 (emphasis added). Although Petitioner argues that, at step 450, the system “authenticate[s] device based on categorization of flagged components” (Pet. 21 (quoting Ex. 1004, 15:42–43)), the quoted text actually refers to step 650 depicted in Etchegoyen’s Figure 6. Figures 4 and 6 depict different embodiments of Etchegoyen’s system. Ex. 1004, 4:16–18, 23–26. Further, Petitioner argues that Etchegoyen’s mini-fingerprints are examples of “data values used to form the response.” Pet. 22; see Ex. 1004, 12:23–27.

Finally, claim 1 recites the step of “recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.” Ex. 1001, 34:44–47. Petitioner argues that Etchegoyen discloses that, “if it is determined that the device has returned an allowable response, then the device ‘may be validly authenticated,’” and “if the device does not return an allowable response, then ‘the device fails [] authentication.’” Pet. 23 (quoting Ex. 1004, 13:22–38).

Petitioner’s mapping of Etchegoyen to independent claims 24 (*id.* at 23–25) and 25 (*id.* at 26–28) is substantially identical to the mapping to claim 1 described above.

ii. *Patent Owner’s Contentions*

Patent Owner contends that Etchegoyen fails to disclose or teach or suggest a system based on “information regarding *anticipated changes to one or more of the stored data values* associated with that identity” and the

step of “determining whether the response is allowable, wherein such determining comprises *using the stored information regarding anticipated changes to the stored data values associated with the identity* to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value.” See Prelim. Resp. 7–11. On this record, we agree.

Initially, Patent Owner notes that Petitioner’s arguments with respect to “anticipated changes” focus on Etchegoyen’s categorization of device components as “typical-upgrade components” and “non-typical-upgrade components.” *Id.* at 7; see Pet. 15–16 (citing Ex. 1004, 4:63–5:2; 13:22–25). Nevertheless, as Patent Owner correctly contends, Etchegoyen does not describe “anticipated changes” to stored data values by use of these categories of components. Prelim. Resp. 7–8. As the Specification of the ’852 patent states, “dynamic key cryptography anticipates changes to computers caused by industry updates to hardware, firmware, and software of computers.” Ex. 1001, 3:15–17. In particular, the Specification describes that:

One embodiment models predictive and anticipated changes that occur naturally and during the use of a computer or device. The larger considered ranges of minutia found on a computer or collected by a computer and the modeled dynamic nature of some minutiae enable a more robust and secure authentication system which is less prone to spoofing.

One embodiment uses a computer identity provider service to collect computer minutia information from the industry and uses this data to anticipate possible changes and permutations to minutiae on registered computers. By anticipating changes in minutiae found on the hardware, firmware, and software elements of a computer, embodiments are more fault-tolerant to natural changes in the computer. *In*

this manner, embodiments can anticipate changes to minutiae and, through a challenge and response exchange between a computer and dynamic key crypto service, synchronize changes to minutiae without actually exchanging the minutiae between the computer and dynamic key crypto service.

Id. at 8:66–9:17 (emphasis added); *see id.*, Fig. 4 (depicting “anticipated changes” stored in Anticipated Minutia DB 98). Thus, we are persuaded that “anticipated changes” refers to predicted or anticipated changes in the stored data values, rather than whether or not a particular component is likely to experience such changes. *See* Prelim. Resp. 8 (“At most, Etchegoyen asserts that upgrades to some types of components are typical, whereas upgrades to other components are non-typical.”; citing Ex. 1004, 5:4–9). In sum, Petitioner has not shown sufficiently that Etchegoyen teaches “such determining comprises using the stored information regarding anticipated changes to the stored data values,” as recited in claim 1.

Moreover, after fingerprint comparison, Etchegoyen may categorize *passing* and *failing* components. As noted above, “each fingerprint portion may be compared against stored fingerprints, flagged as failed or passed, and categorized.” Ex. 1004, 12:55–57. However, Etchegoyen does not rely on this categorization to authenticate the device. As Etchegoyen explains with respect to its Figure 4, “the device may be authenticated solely based on the ratio of passed and failed digital fingerprint portions.” *Id.* at 12:39–41; *see* Pet. 21 (“The system of Etchegoyen performs the claimed determining step by performing steps 420, 430, 440, and 450 of Figure 4.”). Consequently, we are not persuaded that Etchegoyen discloses a system that authenticates a device based on “anticipated changes” in stored data values.

In addition, Petitioner does not demonstrate that Etchegoyen's stored fingerprint information is associated with a component's categorization as typical-upgrade or non-typical-upgrade components. Prelim. Resp. 9–10. As noted above, claim 1 recites that “the information [is] stored for an identity [which] includes (a) *data values associated with that identity*; and (b) *information regarding anticipated changes to one or more of the stored data values associated with that identity*.” Ex. 1001, 34:20–24 (emphases added). Thus, the stored values and the anticipated changes are linked in the recited memory of the claimed system. As Patent Owner explains, however,

[Petitioner] disregards the fact that Etchegoyen does not claim to store information about whether its fingerprints (or fingerprint portions) are on the typical or non-typical upgrade list. [Petitioner] points to a passage in Etchegoyen asserting that the typical/non-typical component categorization is known when the device fingerprints are created (i.e., the “first boot fingerprint”). Etchegoyen at 4:63-5:2 (cited in [Petitioner]'s Petition at 15). But once created, Etchegoyen does not claim to store information about whether a given fingerprint (or fingerprint portion) corresponds to a device on the typical upgrade or non-typical upgrade list. Etchegoyen also never attempts to recategorize its fingerprints/fingerprint portions as corresponding to a particular component on the typical or non-typical upgrade list. And [Petitioner] never asserts or shows how this information is stored with the fingerprint. Pet. at 15-16, 19-20 (element 1.c).

Prelim. Resp. 9–10.

Although Petitioner argues that independent claims 1, 24, and 25 are either anticipated by or rendered obvious over Etchegoyen, Petitioner relies on the same disclosures of Etchegoyen to supply the claim recitations relating to “anticipated changes” in stored data values under either theory of

unpatentability.⁵ Pet. 38 (“Etchegoyen discloses the remaining limitations of Claims 1-5, 7, 14-21, and 24-25 for the reasons recited above in Ground 1.” (emphasis omitted)); see Ex. 1003 ¶ 156. On this record, we are not persuaded that the identified disclosures of Etchegoyen disclose or teach or suggest these limitations of the challenged independent claims relating to “anticipated changes” in stored data values. Thus, for the reasons stated above, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that independent claims 1, 24, or 25 is unpatentable under 35 U.S.C. § 102 or § 103 as anticipated by or rendered obvious over Etchegoyen. Moreover, because each of claims 2–5, 7, and 14–21 depends directly or indirectly from independent claim 1 (Ex. 1001, 34:48–62, 35:1–5, 31–63), we also are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that independent claims 2–5, 7, and 14–21 is unpatentable under 35 U.S.C. § 102 or § 103 as anticipated by or rendered obvious over Etchegoyen.

4. Asserted Obviousness Over Etchegoyen and Jakobsson or Varghese

Petitioner argues that claims 6 and 8–12 are unpatentable under 35 U.S.C. § 103(a) as rendered obvious by the combined teachings of Etchegoyen and Jakobsson (Pet. 38–45) and that claims 13, 22, and 23 are unpatentable under 35 U.S.C. § 103(a) as rendered obvious over the combined teachings of Etchegoyen and Varghese (*id.* at 45–47), and relies upon the testimony of Dr. Traynor to support its arguments (see Ex. 1003

⁵ We note that relying on one disclosure for two elements without sufficient explanation about why both elements are met may not comply with our Rule 42.104(b)(4).

¶¶ 157–184). Each of claims 6, 8–13, 22, and 23 depends directly or indirectly from independent claim 1. Ex. 1001, 34:63–67, 35:6–30, 35:64–36:5.

For the reasons set forth above (*see supra* Section II.B.3.b.), we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that independent claim 1, the base claim for each of these challenged dependent claims, is unpatentable as anticipated by or rendered obvious over Etchegoyen. Moreover, Petitioner does not rely on the teachings of Jakobsson or those of Varghese to supply any of the recited limitations of claim 1 that we found to be missing from Etchegoyen. Therefore, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that any of dependent claims 6, 8–13, 22, and 23 is unpatentable under 35 U.S.C. § 103(a) as rendered obvious over the combined teachings of Etchegoyen and Jakobsson or Varghese.

5. *Asserted Anticipation by and/or Obviousness Over Varghese*

Petitioner argues that claims 1–23 and 25 are unpatentable under 35 U.S.C. § 102(e) or § 102(a) as anticipated by Varghese (Pet. 47–69) and that claim 24 is unpatentable under 35 U.S.C. § 103(a) as rendered obvious over the teachings of Varghese (*id.* at 69–70). Relying on the testimony of Dr. Traynor, Petitioner explains how Varghese allegedly discloses each and every element of claims 1–23 and 25 and how Varghese allegedly teaches or suggests all of the limitations of claim 24. *See* Ex. 1003 ¶¶ 185–246. We begin our analysis with an overview of Varghese.

a. *Varghese (Ex. 1005)*

Varghese is entitled “System and Method for Fraud Monitoring,

Detection, and Tiered User Authentication” (Ex. 1005, [54]) and describes “systems and methods for authenticating access requests from user devices by presenting one of a plurality of graphical user interfaces selected depending on a perceived risk of fraud associated with the devices. User devices are identified with fingerprinting information, and their associated risks of fraud are determined from past experience with the device or with similar devices and from third party information” (*id.* at [57]).

When a request is received from a device or user to access a resource, Varghese’s system issues a “FingerPrintRequest” to the device, which “gathers identifying information describing the device,” such as location information and software information (e.g., OS version). Pet. 11 (citing Ex. 1005 ¶¶ 75, 76, 90). The identity recognition system then analyzes the received minutia values received in response to the “FingerPrintRequest” by comparing them to previously received values. *Id.* Varghese teaches numerous “Security Policies” for analyzing whether or not changes to the minutia are acceptable. *Id.* at 12 (citing Ex. 1005 ¶¶ 98, 100). Using Security Policies, Varghese calculates a risk score for the access request, which is used to determine whether or not to authenticate the device or user. Ex. 1005 ¶¶ 91, 143. One such Security Policy evaluates whether changes show “multiple locations [for a user] over an impossibly short duration of time” because, if so, the user is “likely to be [a] hacker.” Ex. 1005 ¶ 102. Thus, Varghese’s system determines whether to authenticate a device or user by analyzing dynamically changing minutia to “assess[] whether the current behavior is deviating from what is normal[] in similar circumstances.” *Id.* (citing Ex. 1005 ¶¶ 100, 124).

Varghese’s Figure 13B is reproduced below.

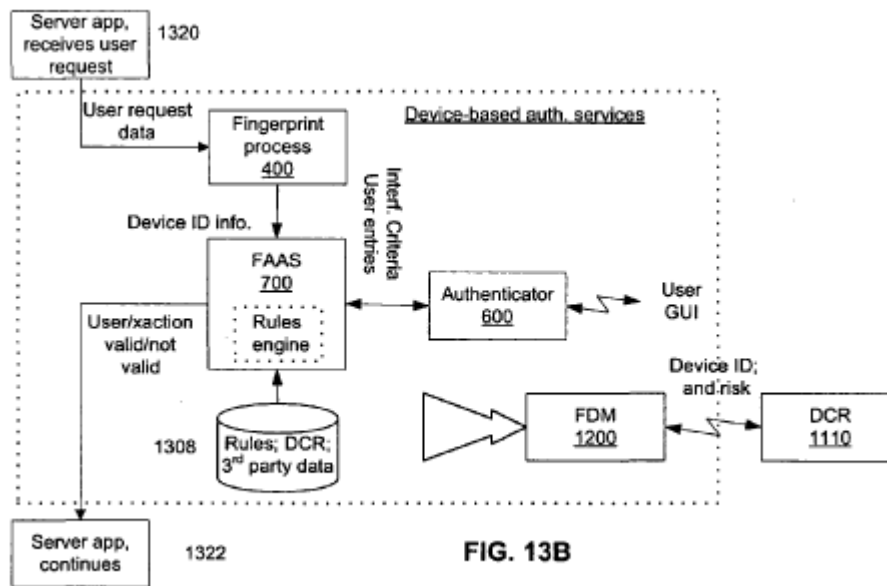


FIG. 13B

Varghese's Figure 13B depicts a system employing computer-implemented processes that cooperate to provide the authentication services, primarily pre-authentication services. Ex. 1005 ¶ 73. The system includes one or more service-provider computer systems, such as systems 1302 and 1304 and authentication system server system 1306, interconnected through network 710 to one or more user devices 720, at which users may logon and enter subsequent access requests. *Id.* ¶ 67. Systems server 1306 includes a CPU, RAM memory, disc or other database memory 1308, communication interfaces, optional user interface equipment, and the like. Database memory 1308 stores data used in the authentication processes, such as device and user histories. *Id.*

Data stored in database memory 1308 also may be third party data. "Third party data can also include IP Intelligence, risk data, historical data (from a data warehouse), fraud network data, and so forth. Further, third party describing characteristics of known risks at the location, device, or user level can be received from third party data warehouses and

incorporating in various fingerprints, primarily the workflow fingerprint and the historical data fingerprint.” *Id.* ¶ 92. “Location information and device information are important criteria, especially in the pre-authentication period. Location information characterizes the location of the device from which a request originates. Location can most easily be estimated from the device’s IP address and the hierarchy of networks linking the device to the Internet.” *Id.* ¶ 93; *see id.*, Table 3 (“Location information”).

Information sources may include device central repository (“DCR”) services, which store the authentication system’s past authentication results, and third party data services, which can provide a wide range of data, such as geolocation data services providing likely geographical source of the current request. *Id.* ¶ 77. A Device ID is usually available and then is the primary item used to identify an authorized user. *Id.* Even when the Device ID is recognized, the user may be required to provide additional security information before being allowed access. *Id.*

When a user knows in advance that a different computer will be used for access at certain times, e.g. business travel to a new location with use of a different computer contemplated, then this information can be provided to the entity and its IP administrator so that the rules for that particular user and time period can be changed to facilitate access to the system and its application. *Id.* ¶ 78.

b. Analysis With Respect to Independent Claims 1 and 25

Petitioner argues that Varghese discloses each and every element recited in independent claim 1. Pet. 47–55. Petitioner applies substantially the same mapping of Varghese to independent claim 25 (*id.* at 55–56). Patent Owner contends, however, that Petitioner’s challenges based on Varghese fail “(1) because Varghese does not have or use information

regarding ‘anticipated changes’; (2) because the allegedly changing data does not come from the device itself, as required by the claim; (3) because the other elements of the dependent claims are not satisfied.”⁶ Prelim. Resp. 20. For the reasons discussed below, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that Varghese discloses each and every element recited in independent claims 1 and 25.

i. Petitioner’s Mapping of Varghese onto Claim 1

Petitioner provides a detailed mapping of the disclosure of Varghese onto the elements of independent claim 1. Pet. 47–55; see Ex. 1003 ¶¶ 185–196. Specifically, Petitioner argues that Varghese discloses a system for authenticating the identity of a device and a user. Ex. 1005 ¶ 65. Similar to the system recited in claim 1, Varghese’s system applies Security Policies that “comprise information about anticipated changes because they include ‘Anomaly detection’ and ‘assess[] whether the current behavior is deviating from what is normally in similar circumstances.’” Pet. 53–54 (citing Ex. 1005 ¶¶ 98, 124). Petitioner argues that Varghese discloses “database 1308[, depicted in Figure 13B,] that contains ‘Rules’ (including Security Policies) and devices central repository (DCR), which ‘gathers the results of the current request authentication processing and stores them . . . in association with the identifying information (for example, the Device ID) for the originating user device.’” *Id.* at 53 (quoting Ex. 1005 ¶ 81). Petitioner

⁶ Because we are not persuaded that Petitioner demonstrates a reasonable likelihood of prevailing in showing that independent claim 1 is unpatentable as anticipated by Varghese, we need not address further the individual challenges to the dependent claims.

argues that database 1308 discloses “a non-transitory memory storing information associated with one or more identities” of the device to be authenticated. *Id.* at 48, 53; see Ex. 1005 ¶ 67.

As noted above, challenged claim 1 recites two types of stored information, namely, “(a) data values associated with that identity; and (b) information regarding anticipated changes to one or more of the stored data values associated with that identity.” Ex. 1001, 34:21–24. Petitioner argues that Varghese stores preferred pre-authentication criteria, which may include location information, and device information, which corresponds to “data values” recited in claim 1. Pet. 48–49 (citing Ex. 1005 ¶¶ 90, 93, Table 3). Further, Petitioner argues that Varghese stores Security Policies, including polies for the detection of anomaly detection. *Id.* at 49 (citing Ex. 1005 ¶¶ 98, 100, 124, Table 5). In particular, Petitioner argues that Varghese discloses that

[a]nother exemplary method is known as “deviation from normal”. This method, instead of comparing current actions to fixed thresholds, employs [] historical data to establish normal for specific days, times, users, devices, workflows, and the like. It then assesses whether the current behavior is deviating from what is normally in similar circumstances.

Ex. 1005 ¶ 124 (emphases added); see Pet. 49, 53–54.

Claim 1 further recites “one or more hardware processors in communication with the memory and configured to execute instructions to cause the identity recognition system to recognize that the presentation of identity information by a computer is authentic, by performing operations.” Ex. 1001, 34:25–29. Petitioner argues that, referring to its Figure 13B, Varghese discloses “processors that perform ‘device-based authentication

services’ including a Rules Engine and Authenticator,” which perform steps as recited in claim 1. Pet. 54 (citing Ex. 1005 ¶ 97).

Claim 1 recites four method steps performed by the “one or more hardware processors.” Ex. 1001, 34:30–47. Petitioner argues that Varghese discloses each of these steps. Specifically, claim 1 recites the step of “generating a challenge to the computer, wherein the challenge prompts the computer to provide a response based on one or more data values from the computer that correspond to one or more of the stored data values associated with the identity.” *Id.* at 34:30–34. In view of the agreed construction of the term “generating a challenge” (*see supra* Section II.A.1.), Petitioner argues that Varghese discloses “generating a challenge in the form of a ‘FingerPrintRequest,’” which corresponds to the recited challenge. Pet. 54 (citing Ex. 1005 ¶¶ 74, 75, Fig. 13B). Referring to Figure 13B, Varghese discloses that user request 1320 is received by server application or services provider computer system, and authentication services are invoked through an externally available, application programming interface (“API”). Ex. 1005 ¶¶ 74, 75, Table 1. Varghese’s Table 1, reproduced below,

TABLE 1				
<u>Example API requests</u>				
#	Description	Action	Request XML	Response XML
1	Pre-authentication request to fingerprint the device	FingerPrintRequest	FingerPrintRequest.xml	FingerPrintResponse.xml
2	Updates the authentication status for the authentication session	UpdateAuthResult	UpdateAuthResultRequest.xml	FingerPrintResponse.xml
3	Processes the rules	ProcessRules	ProcessRulesRequest.	ProcessRulesRespon

lists exemplary APIs including “FingerPrintRequest” and “FingerPrintResponse.” *See id.* ¶ 76 (“Fingerprint process 400 is the first authentication process invoked with input data describing the user request. The fingerprint process then gathers identifying information describing the

device from which the user request originated and creates a device identifier (“Device ID”). The Device ID (and optionally other device identifying information) is stored on the user device from which it can be retrieved and form part of the device identifying information to be used during a subsequent fingerprinting.”).

Claim 1 further recites the step of “receiving, from the computer, the response to the challenge.” Ex. 1001, 34:35–36. Referring to Varghese’s Table 1, Petitioner argues that Varghese discloses a “FingerPrintResponse.” Pet. 54. This API is part of fingerprinting process 400 which “capture[s] identity information from user device.” *Id.*; see Ex. 1005, Fig. 4 (step 404).

Claim 1 further recites “determining whether the response is allowable, wherein such determining comprises using the stored information regarding anticipated changes to the stored data values associated with the identity to determine whether a data value used to form the response is based on an acceptable change to a corresponding stored data value.” Ex. 1001, 34:37–43. Petitioner argues that the security policies depicted in Varghese’s Figures 15A and 15B, which depict “an exemplary policy set and an exemplary security model for inclusion within the exemplary policy set,” disclose this element. Pet. 51–52. Referring to Figure 15B, Varghese discloses that “an exemplary set of such data items. For example, a user who submits requests that appear to originate from multiple machines, or multiple cities, or multiple locations over an impossibly short duration of time has been found likely to be [a] hacker.” Ex. 1005 ¶ 102. Specifically, Petitioner argues that:

For example, *Varghese* discloses determining whether the response is allowable using Security Policies (information regarding anticipated changes). One example policy evaluates

whether a change in device location is acceptable based on the period of time between when the device was observed at successive locations. If the device or user has been observed in “multiple locations over an impossibly short duration of time,” this constitutes an unacceptable change and the system determines the user is a likely hacker. *Id.*, ¶0102. A [person of skill in the art] would understand from the disclosure of Varghese that if the duration of time is outside a pre-determined threshold, however, this security policy is not triggered and the device/user may be authenticated. IA1003, ¶195.

Pet. 55 (emphasis added); see Ex. 1005 ¶¶ 103 (Table 6A: “Restricted model”), 104 (Table 6B: “Hacker model”).

Finally, claim 1 recites the step of “recognizing that the presentation of identity information by the computer is authentic, according to whether the computer has provided an allowable response to the challenge.”

Ex. 1001, 34:44–47. Petitioner argues that Varghese discloses that, “[e]ither the rules engine, or the service provider application, or both together evaluate the user authentication information to determine whether or not the user is authenticated.” Pet. 55 (quoting Ex. 1005 ¶ 143).

Petitioner’s mapping of Varghese to independent claim 25 (*id.* at 55–56) is substantially identical to the mapping to claim 1 described above.

ii. *Patent Owner’s Contentions*

As noted above, Patent Owner contends that (1) because Varghese does not have or use information regarding “anticipated changes,” i.e., location information, to formulate the device’s response and (2) because the allegedly changing data, i.e., location information, comes from third parties, rather than from the device itself; Varghese does not disclose each and every element recited in claim 1. Prelim. Resp. 22–25. On this record, we agree.

First, Patent Owner notes that, in the examples on which Petitioner relies, Varghese “rejects access attempts from ‘a user who has ‘submit[ed] requests that appear to originate from . . . multiple locations over an impossibly short duration of time.’” Pet. 54 (quoting Ex. 1005 ¶ 102). This analysis, however, is not based on *anticipated* changes. Prelim. Resp. 22. Instead, it is based on location data received or derived from a third party with a prescribed time window. *Id.*; see Ex. 1005 ¶¶ 77, 140, 169, 181. If the received location data is not sufficiently proximate or not sufficiently separated in time, access is denied. See Ex. 1005 ¶ 102. Thus, in order to result in access denial, the received data need not be *anticipated* or even accurate, it need only be sufficiently different.

Second, Patent Owner contends that Petitioner’s arguments rely exclusively on Varghese’s assessment of data values regarding “location” information. Pet. 55. However, Varghese does not disclose that the location information is part of “a response *based on one or more data values from the computer that correspond to one or more of the stored data values* associated with the identity.” Ex. 1001, 34:31–34 (emphasis added). Specifically, Petitioner argues that the “response” is provided by Varghese’s “FingerPrintResponse.xml” functionality which “capture[s] identity information from the user device.” Prelim. Resp. 23 (citing Pet. 54 (quoting Ex. 1005, Fig. 4 (step 402))). Thus, Patent Owner contends that

in Varghese, location information is not submitted as part of the “response” and thus cannot provide the predicate for “determining . . . whether a data value used to form the response is based on an acceptable change to a corresponding stored data value.” ’852 patent, claim 1 (emphasis added).

The reason that location information is not part of the response is simple—in Varghese, location information is not provided by the device, but instead is provided by a third party. *Id.* at 24. Because Petitioner’s anticipation arguments with respect to Varghese rely on Varghese’s use of location information and because Varghese discloses location information obtained from third parties (Ex. 1005 ¶¶ 77, 140, 169, 181) or *in advance* from the user (*id.* ¶ 78), we are not persuaded that Petitioner demonstrates that the location information is part of the response, as recited in the “generating” step or is used as part of the “determining” step of challenged claim 1. Prelim. Resp. 25.

On this record and for the reasons stated above, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that independent claim 1 or 25 is unpatentable under 35 U.S.C. § 102 as anticipated by Varghese. Moreover, because each of claims 2–23 depends directly or indirectly from independent claim 1 (Ex. 1001, 34:48–36:5), we also are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that any of dependent claims 2–23 is unpatentable under 35 U.S.C. § 102 as anticipated by Varghese.

6. *Asserted Obviousness Over Varghese*

Petitioner argues that independent claim 24 is unpatentable under 35 U.S.C. § 103(a) as rendered obvious by the teachings of Varghese (Pet. 69–70), and relies upon the testimony of Dr. Traynor to support its arguments (see Ex. 1003 ¶¶ 236–246). In particular, Petitioner argues that “Varghese discloses limitations 2[5].a-25.d and 25.f-25.h. and any limitations found to be present in the preamble.” Pet. 69 (citing Ex. 1001, 34:18–47 (claim 1)). Unlike claim 25, however, claim 24 recites “generating a challenge, wherein

the challenge originates at the computer and prompts the computer to transmit an identity claim comprising identity information.” Ex. 1001, 36:16–18 (emphasis added). Petitioner argues that this is a trivial modification to the system taught by Varghese for a person of ordinary skill in the art to implement. Pet. 69. Moreover,

[a person of ordinary skill in the art] would have reason to make this modification to, *inter alia*, reduce the number of communications between the computer and server. A [person of ordinary skill] would expect success with this approach as it simply changes where the API is called but does not alter the underlying functionality of the system. IA1003, ¶¶241-242.

Pet. 70.

For the reasons set forth above (*see supra* Section II.B.5.b.), we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing in showing that independent claims 1 and 25 are unpatentable as anticipated by Varghese. Moreover, Petitioner does not rely on modifications to the teachings of Varghese to supply the recited limitations of claim 24 that we found to be missing from Varghese’s disclosure with respect to claims 1 and 25. Therefore, we are not persuaded that Petitioner has shown a reasonable likelihood of prevailing in its assertion that independent claim 24 is unpatentable under 35 U.S.C. § 103(a) as rendered obvious over the teachings of Varghese.

III. CONCLUSION

After consideration of the Petition, the Preliminary Response, and the supporting evidence, we are not persuaded that Petitioner demonstrates a reasonable likelihood of prevailing in showing that at least one of claims 1–25 of the ’852 patent is unpatentable on any of the asserted grounds. On this

record, we *deny* institution of *inter partes* review of claims 1–25 of the '852 patent.

IV. ORDER

Accordingly, it is:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review is *denied* with respect to claims 1–25 of the '852 patent on the asserted grounds.

For PETITIONER:

Peter J. Armenio
Matthew D. Robson
QUINN EMANUEL URQUHART & SULLIVAN LLP
peterarmenio@quinnemanuel.com
matthewrobson@quinnemanuel.com

For PATENT OWNER:

Thomas B. King
Kenneth G. Parker
Jason T. Lao
HAYNES AND BOONE, LLP
thomas.king@haynesboone.com
kenneth.parker@haynesboone.com
jason.lao@haynesboone.com