

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

IDENTITY SECURITY LLC,
Patent Owner.

IPR2022-00172
Patent 8,489,895 B2

Before BARBARA A. PARVIS, CHRISTOPHER L. OGDEN, and
SHARON FENICK, *Administrative Patent Judges*.

PARVIS, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Apple Inc. (“Petitioner”) filed a Petition (Paper 1 (“Pet.”)) requesting *inter partes* review of claims 1, 2, 4, 5, 7, 8, 10, 13, and 14 (“challenged claims”) of U.S. Patent No. 8,489,895 B2 (Ex. 1001, “the ’895 patent”), along with the supporting Declaration of Clifford Neuman, Ph.D. (Ex. 1003). Identity Security LLC (“Patent Owner”) filed a Preliminary Response (Paper 8 (“Prelim. Resp.”)), along with the supporting Declaration of Samuel Russ, Ph.D. (Ex. 2001).

The standard for institution is set forth in 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition and the Preliminary Response shows that “there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314; *see also* 37 C.F.R. § 42.4(a) (“The Board institutes the trial on behalf of the Director.”). Upon consideration of the parties’ contentions and the evidence of record, we conclude that Petitioner has not established a reasonable likelihood of prevailing in demonstrating the unpatentability of any challenged claim of the ’895 patent. Accordingly, we do not grant Petitioner’s request and do not institute an *inter partes* review.

II. BACKGROUND

A. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), the parties inform us that the ’895 patent is involved in the following district court case: *Identity Security LLC v. Apple Inc.*, No. 6:21-cv-00460 (W.D. Tex.). Pet. 52, Paper 5, 1. Patent Owner also asserts that a decision in this proceeding could affect or be affected by the following judicial matter: *Identity Security LLC v. Apple Inc.*, No. 1:22-cv-00058 (W.D. Tex.). Paper 5, 1.

Petitioner also has contemporaneously filed petitions for review of related patents as follows: (1) a petition for *inter partes* review of U.S. Patent No. 7,493,497 B1 (IPR2022-00170); (2) a petition for *inter partes* review of U.S. Patent No. 8,020,008 B2 (IPR2022-00171); and (3) a petition for *inter partes* review of U.S. Patent No. 9,507,948 B2 (IPR2022-00173).

B. The '895 Patent

The '895 patent relates to a digital identity device for uniquely identifying legal entities. Ex. 1001, code (57). A digital identity device is shown below in Figure 2.

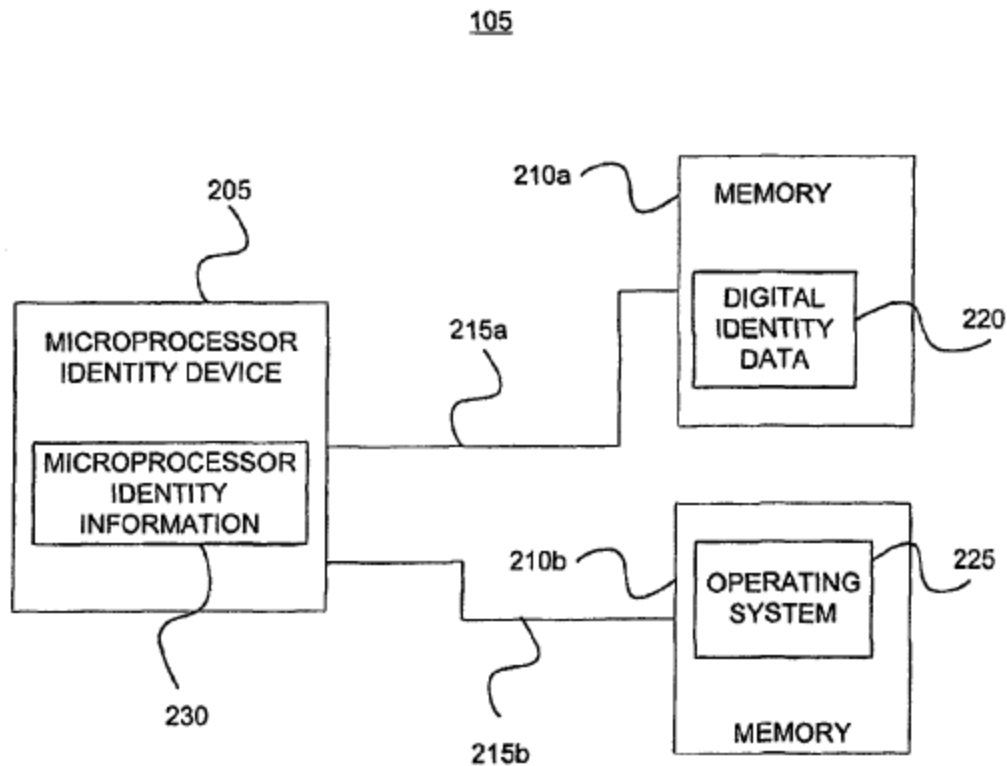


Fig. 2



Figure 2, above, illustrates a schematic view of digital identity device 105 including microprocessor identity device 205, first memory 210*a*, second memory 210*b*, and communication interfaces 215 for coupling microprocessor identity device 205 to memories 210. *Id.* at 2:34–35, 3:60–65, 4:25–26.

Microprocessor identity device 205 includes microprocessor identity information 230. *Id.* at 3:66–67. Microprocessor identity information 230 is unique to microprocessor identity device 205 and distinguishes microprocessor identity device 205 from other microprocessor devices. *Id.* at 4:1–4.

First memory 210*a* and second memory 210*b* are any commercially available memory, such as non-volatile random access memory (NVRAM). *Id.* at 4:21–23. First memory 210*a* includes digital identity data 220. *Id.* at 4:26–27. Digital identity data 220 is etched onto first memory 210*a* using any conventional etching method. *Id.* at 4:27–28. Digital identity data 220 is for an individual or a corporation. *Id.* at 4:28–29. Digital identity data 220 includes one or more of the following: a name, a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, a digital thumb print, a DNA code, one or more credit cards' information, one or more bank accounts' information, an incorporation name, a date and a place of incorporation, one or more corporate officers, one or more corporate partners, or one or more D.B.A. names. *Id.* at 4:30–37.

Second memory 210*b* includes operating system 225. *Id.* at 4:38–39. Operating system 225 binds digital identity data 220 to microprocessor identity device 205 by encoding digital identity data 220 with passwords input by an owner of digital identity device 105. *Id.* at 4:40–42. Digital

identity data 220 is encoded by an algorithm that uses microprocessor identity information 230. *Id.* at 4:42–44.

C. Illustrative Claim

Petitioner challenges claims 1, 2, 4, 5, 7, 8, 10, 13, and 14 of the '895 patent. Pet. 1. Claims 1, 4, 5, 7, and 10 are the independent claims. Claim 2 depends directly from claim 1. Claim 8 depends directly from claim 7. Claim 13 depends directly from claim 4 and claim 14 depends directly from claim 5. Independent claim 1, reproduced below, is illustrative of the claimed subject matter.

1. [1(P)]¹ A microprocessor identity device, comprising:
 - [1(a)] a microprocessor;
 - [1(b)] microprocessor identity information that uniquely identifies the microprocessor identity device; and
 - [1(c)] digital identity data that identifies an owner of the microprocessor identity device, [1(d)] the digital identity data being bound to the microprocessor identity device,wherein when the owner provides the digital identity data, the digital identity data is bound to the microprocessor identity device by encryption of the digital identity data with the microprocessor identity information to thereby establish the owner's ownership of the microprocessor identity device.

Ex. 1001, 11:63–12:10.

D. Evidence

Petitioner relies on the patent document references summarized below.

Name	Patent Document	Exhibit
Gullman	US 5,280,527, issued Jan. 18,	1004

¹ We use Petitioner's designations to refer to the elements of the claim. Pet. 11–17.

	1994	
Laczko	EP 0961193 A2, published Dec. 1, 1999	1005
Padgett	US 6,167,518, issued Dec. 26, 2000	1006

E. Asserted Grounds

Petitioner asserts that the challenged claims of the '895 patent are unpatentable based on the following grounds summarized below:

Claims Challenged	35 U.S.C. §²	References/Basis
1, 2, 4, 7, 10, 13	103(a)	Gullman, Laczko
1, 2, 4, 5, 7, 8, 10, 13, 14	103(a)	Gullman, Laczko, Padgett

III. ANALYSIS

A. Legal Standards

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) as “requiring [*inter partes* review] petitions to identify ‘with particularity . . . the evidence that supports the grounds for the challenge to each claim’”); *see also* 37 C.F.R. § 42.104(b) (requiring a petition for *inter partes* review to identify how the challenged claim is to be construed and where each element of the claim is found in the

² Because the challenged claims of the '895 patent have an apparent effective filing date before March 16, 2013, the 35 U.S.C. §§ 102 and 103 provisions of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, §§ 3(b)–3(c), 3(n)(1), 125 Stat. 284, 285–87, 293 (2011) do not apply and we apply the pre-AIA versions of these statutes. Our application of the pre-AIA law is not an affirmative ruling on the actual effective filing date of this patent.

prior art patents or printed publications relied upon). That burden never shifts to the patentee. *Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015). Furthermore, Petitioner cannot satisfy its burden of proving obviousness by employing “mere conclusory statements.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

A patent claim is unpatentable under 35 U.S.C. § 103 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). The question of obviousness 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; and (4) when in evidence, objective evidence of obviousness or nonobviousness.³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Petitioner asserts a “person having ordinary skill in the art (“PHOSITA”) at the time of the ’895 Patent would have had at least a bachelor’s degree in computer science or equivalent with at least one year of experience in the field of computer security and encryption.” Pet. 3–4 (citing Ex. 1003 ¶¶ 24–26). Petitioner also asserts “[a]dditional education or experience might substitute for the above requirements.” *Id.* at 4. Patent Owner does not dispute the qualifications of a person having ordinary skill in the art proposed by Petitioner. Prelim. Resp. 6.

³ The parties did not present evidence of secondary considerations.

On the current record, we find Petitioner’s contentions that the skilled artisan would have had “*at least* a bachelor’s degree” and “*at least* one year” of experience to be too vague as Petitioner’s contentions encompass skill levels beyond the proposal level without a defined limit. We, therefore, adopt Petitioner’s proposal except we do not adopt the “at least” terminology above. We determine that with our changes Petitioner’s proposal is consistent with the level of skill reflected in the ’895 patent Specification and the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

C. Claim Construction

We construe the challenged claims by applying the standard used in federal courts, in other words, “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b),” which is articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b) (2021). For the reasons provided below, we do not discern a need to construe explicitly any claim terms because doing so would not change the outcome of the analysis below. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (stating that “we 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))).

D. Obviousness over Gullman and Laczko—Claims 1, 2, 4, 7, 10, and 13

Petitioner asserts that claims 1, 2, 4, 7, 10, and 13 would have been obvious over Gullman and Laczko. Pet. 4. Patent Owner disputes

Petitioner's showing. *See, e.g.*, Prelim. Resp. 27–36. We begin with summaries of Gullman and Laczko and then we turn to the parties' dispute.

1. Gullman

Gullman relates to an apparatus for accepting a biometric measurement, which is then used as a seed for deriving a security token. Ex. 1004, 1:8–11. A security system including a biometric security apparatus for generating a token is shown below in Figure 1. *Id.* at 3:8–10.

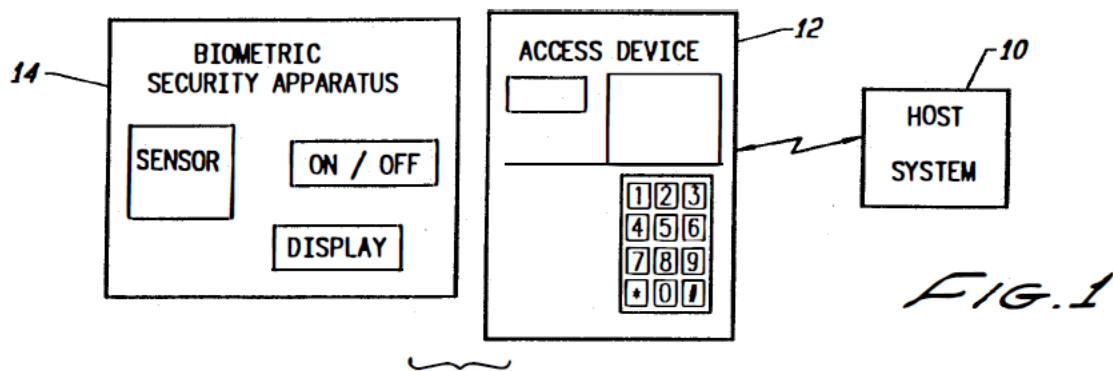


Figure 1, above, illustrates a block diagram of a security system including access device 12 and biometric security apparatus 14 for providing security safeguards for accessing host system 10. *Id.* at 3:18–21.

Host system 10 is a computer system containing confidential or valuable information that must be secured against unauthorized access, such as an on-line bank system. *Id.* at 3:19–24. To safeguard access to such information, access is limited by access device 12. *Id.* at 3:24–26. Access device 12 communicates with host system 10 to verify authorized personnel and transfer information. *Id.* at 3:26–29. Access device 12 may be, for example, a terminal in communication with a host computer or an automated teller machine in communication with a banking network. *Id.* at 3:28–32.

Biometric security apparatus 14 generates a security token, which a user inputs to access device 12. *Id.* at 3:37–39, 6:35–37. To generate a security token, biometric security apparatus 14 receives biometric input and then compares the biometric input to a stored template to derive a correlation factor. *Id.* at 3:44–46, 6:10–20. Biometric input may be a fingerprint, voiceprint, or writing sample. *Id.* at 3:42–44. If the correlation factor is below a prescribed threshold, the correlation is unsuccessful. *Id.* at 3:46–48, 6:20–22. For a successful biometric entry, the correlation factor is combined with a fixed code and a time-varying code to generate the security token. *Id.* at 4:3–8, 6:30–34. The user then enters the security token at access device 12. *Id.* at 4:12–13, 6:35–37. Access device 12 sends the token to host 10, which decodes the token. *Id.* at 4:13–14, 6:37–39.

To decode the security token biometric security apparatus 14 is synchronized with host 10 so that the time varying code is identical at both biometric security apparatus 14 and host 10. *Id.* at 4:23–26. Host 10 identifies the user with the fixed code and verifies the identification based on the correlation factor. *Id.* at 4:29–31, 6:38–42.

2. *Laczko*

Laczko relates to secure computing systems that execute after manufacture field provided programs secured to prevent the user from unauthorized use of selected computer services. Ex. 1005 ¶ 1. *Laczko* describes the following:

The data processor is disposed on a single integrated circuit. This data processor includes a chip identity read only register storing a unique chip identity number. This unique chip identity number is fixed during manufacture by, for example, laser probing or selective activation of fuse or antifuse links in the chip identity register. The data processor encrypts the

compressed video data stream using at least a part of the chip identity number as an encryption key.

Id. at ¶ 11.

3. *Independent Claim 1*

a) *Petitioner's Showing for Element 1(d) is Insufficient*

Element 1(d) recites the following:

[1(d)] the digital identity data being bound to the microprocessor identity device,

wherein when the owner provides the digital identity data, the digital identity data is bound to the microprocessor identity device *by encryption of the digital identity data* with the microprocessor identity information to thereby establish the owner's ownership of the microprocessor identity device.

Ex. 1001, 12:2–10 (emphasis added). The parties dispute whether the asserted prior art teaches encrypting digital identity data.

Petitioner relies on Gullman's teachings for most elements recited in claim 1 including the recitation of "digital identity data" in element 1(c) and the requirement that the "digital identity data is bound to the microprocessor identity device by encryption of the digital identity data with the microprocessor identity information" in element 1(d). Pet. 11–25. Petitioner relies on Laczko's teachings only for asserting that use of the microprocessor identity information as the encryption key was known, which is not pertinent to the dispute we consider here. *Id.* at 23–25.

Petitioner asserts that Gullman teaches recitation 1(d) because Gullman uses an algorithm to encrypt "biometric input (digital identity data) in order to generate a token." *Id.* at 18. Petitioner points to (*id.* at 19) Gullman's "BACKGROUND OF THE INVENTION," which discloses that "a password (fixed key) is encoded based on time-variant information."

Ex. 1004, 1:34–45. Petitioner asserts that Gullman “uses this same encoded token process, but further proposes a security apparatus that receives ‘biometric information is input to . . . generate[] . . . a security token’ where ‘[t]he biometric information is used as part of the “seed” for generating the token.’” Pet. 19 (quoting Ex. 1004, 2:20–23).

Petitioner asserts that a person having ordinary skill in the art would have understood that Gullman “is describing an encryption process” and Gullman describes using “encryption to generate tokens.” *Id.* at 20–21 (citing, *e.g.*, Ex. 1003 ¶¶ 65–66). Petitioner asserts that “[i]n some embodiments, *Gullman*’s security tokens are generated using the owner’s biometric input from biometric sensor 18 and the fixed code.” *Id.* at 21–22 (citing Ex. 1004, 2:55–59, 3:39–41, 5:11–14). Petitioner asserts “[i]n other embodiments, Gullman teaches that the security token is generated from the correlation factor that results from a comparison of the inputted biometric data and stored biometric template.” *Id.* at 22 (citing Ex. 1004, 6:12–42). Petitioner does not argue that Gullman’s disclosure of generating a security token from the correlation factor teaches element 1(d). *Id.* To the contrary, Petitioner relies on its alternative ground of obviousness over Gullman, Padgett, and Laczko if a determination is made that “*Gullman*’s token always includes the correlation factor.” *Id.*

Dr. Neuman testifies “Gullman teaches in some embodiments [that] its security tokens are generated using the owner’s biometric input from biometric sensor 18, a time-varying code, and the fixed code.” Ex. 1003 ¶ 65 (citing Ex. 1004, 5:11–14). Dr. Neuman’s testimony relies on only one disclosure in Gullman, which is the same as a disclosure identified by Petitioner. *Id.*

Patent Owner asserts “Gullman does not teach encrypting the biometric input,” but, instead “Gullman teaches encrypting a biometric correlation factor (also referred to as a ‘verification’) as part of a token.” Prelim. Resp. 27 (citing Ex. 2001 ¶ 84; Ex. 1004, code (57)). Patent Owner asserts “[w]hile the correlation factor is calculated *based on* the biometric input, the biometric input itself is not included in the security token and therefore not encrypted.” *Id.* Dr. Russ testifies that a person having ordinary skill in the art would not have understood Gullman “to teach including the biometric input in the security token or encrypting it.” Ex. 2001 ¶ 84 (citing, *e.g.*, Ex. 1004, 5:15–19).

We agree with Patent Owner that Petitioner has not shown Gullman teaches encrypting biometric information. We credit Dr. Russ’s testimony over Dr. Neuman’s testimony as Dr. Russ’s testimony is consistent with the evidence of record. That biometric information is received and used to generate security tokens does not mean that Gullman’s security tokens include biometric information or that any biometric information is encrypted.

We start with Petitioner’s assertion that Gullman “proposes a security apparatus that receives ‘biometric information is input to . . . generate[] . . . a security token’ where ‘[t]he biometric information is used as part of the “seed” for generating the token.’” Pet. 19 (quoting Ex. 1004, 2:20–23). Gullman further discloses that “the user enters . . . biometric information to the security mechanism” and “[t]he mechanism verifies the input against the template, then generates and displays a token *based on the verification*.” Ex. 1004, 2:31–35 (emphasis added). Gullman discloses “[m]ore specifically, the *token is derived from the results of the biometric comparison*, plus a time-varying value.” *Id.* at 2:37–39.

That biometric information is input and “used as part of the ‘seed’ for generating the token” does not mean that the token includes biometric information or that biometric information is encrypted. *Id.* at 2:20–23. Gullman’s disclosure that the mechanism “generates and displays a token *based on the verification*” (*id.* at 2:31–35 (emphasis added)) and that “the token is derived from the results of the *biometric comparison*” (*id.* at 2:37–39 (emphasis added)) indicate that contrary to Petitioner’s assertion the biometric information is used only in a comparison. Gullman’s disclosures do not teach generating a security token that includes biometric information that is then encoded or encrypted.

We turn to Petitioner’s assertion that Gullman’s security token includes biometric information because “[i]n some embodiments, *Gullman’s* security tokens are generated using the owner’s biometric input from biometric sensor 18 and the fixed code.” Pet. 21–22 (citing Ex. 1004, 2:55–59, 3:39–41, 5:11–14). In the first of the disclosures relied on by Petitioner, Gullman states “[u]pon entry of the cardholder’s biometric information, the processor executes the verification algorithm. The verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number) and time-varying self-generated information to derive a token output.” Ex. 1004, 2:53–59. Mere use of biometric input by a verification algorithm does not teach generating a security token that includes biometric information that is then encoded or encrypted.

Furthermore, Gullman describes that its verification algorithm uses a correlation factor. In particular, Gullman describes the following:

A correlation factor is calculated for each template. If the correlation factor indicates correlation closer than a prescribed threshold level (i.e., 90 on a scale of 0 to 100) for any template,

then the biometric *verification* is successful. If none of the correlation factors satisfy the prescribed level, then the biometric *verification* is unsuccessful.

Ex. 1004, 6:16–22 (emphases added). Gullman’s correlation factor is simply a factor, such as 90 on a scale of 0 to 100, indicating the degree of correlation between biometric input provided to Gullman’s biometric security apparatus and one or more templates stored by the biometric security apparatus. *Id.* at 6:12–22. Gullman does not teach or suggest the use of the biometric input by the access device 12 or host system 10.

In the second of the disclosures relied on by Petitioner (Pet. 21–22), Gullman states “[s]uch security token is formed from biometric information, a fixed code and, in one embodiment, a time-varying code or, in a second embodiment, a host-generated challenge code.” Ex. 1004, 3:39–42.

Gullman’s full disclosure is that “[t]he security apparatus 14 receives the biometric input, then compares the biometric input to a stored template to derive a correlation factor. If the correlation factor is below a prescribed threshold level, the correlation is unsuccessful.” *Id.* at 3:44–48. Gullman further discloses that, “[f]or a successful biometric entry . . . , the correlation factor is combined with a fixed code (i.e., PIN, embedded serial number, account number) and in one embodiment, a time-varying code (i.e., the time of day) to generate the security token.” *Id.* at 4:3–8. That the security token is “formed from biometric information” is not sufficient to show that the security token includes biometric information that is then encoded or encrypted. Furthermore, here Gullman’s immediately subsequent disclosures clarify that “formed from” merely indicates that the biometric input is used to derive a correlation factor that is combined with the fixed code and time-varying code to generate the security token. *Id.* at 3:39–41, 3:44–48, 4:3–8.

In the third of the disclosures relied on by Petitioner (Pet. 21–22), which was cited by Dr. Neuman (Ex. 1003 ¶ 65), Gullman states “[p]rocessor 22 generates a security token based on the time-varying code, fixed code and biometric input from biometric sensor 18, and outputs the token to display 20.” Ex. 1004, 5:11–14. Petitioner characterizes Gullman’s disclosure of generating a security token “based on” biometric input as a “primary” embodiment. Pet. 21. The description of generating a security token “based on” the biometric input encompasses generating a security token having a correlation factor that is derived as the result of the comparison.

Petitioner asserts that Gullman describes an “alternative” embodiment that “differs in that it relies on a distinct encryption ‘module’ to encrypt the timestamp, biometric data, and the fixed code.” *Id.* Consistent with Patent Owner’s contentions and Dr. Russ’s testimony, however, Gullman’s full disclosure is that “[a]lternatively, processor 20 may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock 25, the fixed code and *a biometric correlation factor*, generating an encrypted security token.” Ex. 1004, 5:15–19 (emphasis added). Although Gullman describes that “alternatively” a standard encryption module is included, Gullman does not describe an alternative embodiment that involves generating security tokens differently. *Id.* at 5:2–19.

We credit Dr. Russ’s testimony over Dr. Neuman’s testimony as Dr. Russ’s testimony is consistent with the evidence of record. Dr. Russ’s testimony that a person having ordinary skill in the art would not have understood Gullman “to teach including the biometric input in the security token or encrypting it” (Ex. 2001 ¶ 84 (citing, *e.g.*, Ex. 1004, 5:15–19)) is

consistent with Gullman’s disclosure that the encryption module “applies an encryption algorithm to the time of day from real time clock 25, the fixed code and *a biometric correlation factor*, generating an encrypted security token.” Ex. 1004, 5:15–19 (emphasis added).

Dr. Neuman’s testimony cites only Gullman’s disclosure of generating a security token “based on” biometric input (Ex. 1003 ¶ 65 (citing Ex. 1004, 5:11–14)), which encompasses generating a security token having a correlation factor that is derived as the result of a comparison. Petitioner discusses the disclosures relied on by Dr. Neuman and Dr. Russ and asserts only one difference, i.e., “that the ‘alternative’ embodiment differs in that it relies on a distinct encryption ‘module’” to perform the encrypting. Pet. 21 (citing Ex. 1003 ¶¶ 65–66). We give Dr. Neuman’s testimony that “*Gullman* teaches that in some embodiments its security tokens are generated using the owner’s biometric input from biometric sensor 18, a time-varying code, and the fixed code” (Ex. 1003 ¶ 65) little or no weight because his testimony does not disclose underlying facts or data that support sufficiently the opinion. *See* 37 C.F.R. § 42.65(a) (“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight”).

In sum, Petitioner’s showing is deficient because in Gullman any encoding or encryption is of a security token that is generated by combining the result of a comparison, in particular a correlation factor, with other non-biometric data, such as a fixed code and a time-varying code. Petitioner’s reliance on “some embodiments” in which “*Gullman*’s security tokens are generated using the owner’s biometric input from biometric sensor 18 and the fixed code” (Pet. 21–22) is misplaced and does not consider the full disclosures of Gullman that describe that even in those embodiments the

biometric data is used merely in a comparison and is not included in a security token and encoded or encrypted.

Petitioner does not rely on Laczko for teaching encrypting digital identity data in element 1(d). Also, upon consideration, Laczko's teachings relied on by Petitioner do not remedy the aforementioned deficiency.

We, therefore, determine Petitioner has not shown sufficiently that the combination of Gullman and Laczko teaches element 1(d).

b) Conclusion—Obviousness of Claim 1 over Gullman and Laczko

After consideration of the contentions and the evidence of record, we determine that Petitioner has not shown sufficiently that the combination of Gullman and Laczko teaches each recitation of claim 1. Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claim 1 is unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman and Laczko.

4. Independent Claims 4, 7, and 10

Each of independent claims 4, 7, and 10 includes a recitation that similar to element 1(d) that requires encrypting digital identity data. *See* Ex. 1001, 12:38–40 (recitation in claim 4 requiring that “the digital identity data is bound to the microprocessor identity device by encryption of the digital identity data with the microprocessor identity information”), 12:62–64 (recitation in claim 7 requiring “the digital identity data being encrypted with an algorithm that uses the microprocessor identity information”), 13:7–10 (recitation in claim 10 requiring “the digital identity data being encrypted with the microprocessor identity information when the owner establishes ownership of the microprocessor identity device”). For these recitations, Petitioner relies on its arguments and evidence for element 1(d) without

supplementation. Pet. 29–30. Petitioner’s showing for the aforementioned elements is not sufficient for the same reasons given for claim 1. *See supra* § III.D.3.

For the reasons given for claim 1, we determine that Petitioner has not shown sufficiently that the combination of Gullman and Laczko teaches each recitation of claims 4, 7, and 10. Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 4, 7, and 10 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman and Laczko.

5. *Dependent Claims 2 and 13*

Claim 2 depends directly from claim 1 and claim 13 depends directly from claim 4. Petitioner’s arguments and evidence for dependent claims 2 and 13 do not remedy the deficiencies discussed with respect to claims 1 and 4. Pet. 25–26, 30.

Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 2 and 13 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman and Laczko.

E. *Obviousness over Gullman, Laczko, and Padgett—
Claims 1, 2, 4, 5, 7, 8, 10, 13, and 14*

Petitioner asserts that claims 1, 2, 4, 5, 7, 8, 10, 13, and 14 would have been obvious over Gullman, Laczko, and Padgett. Pet. 4. Patent Owner disputes Petitioner’s showing. *See, e.g.*, Prelim. Resp. 36–48. We begin with a summary of Padgett. We then turn to the parties’ dispute.

1. *Padgett*

Padgett relates to the field of authentication of electronic documents, and more particularly to a non-reputable digital signature that allows

authentication of the identity of the sender of a message by comparison with the sender's unique biological indicia. Ex. 1006, 1:6–11. Figure 1, below, shows a terminal used for forming a digital certificate. *Id.* at 3:49–51.

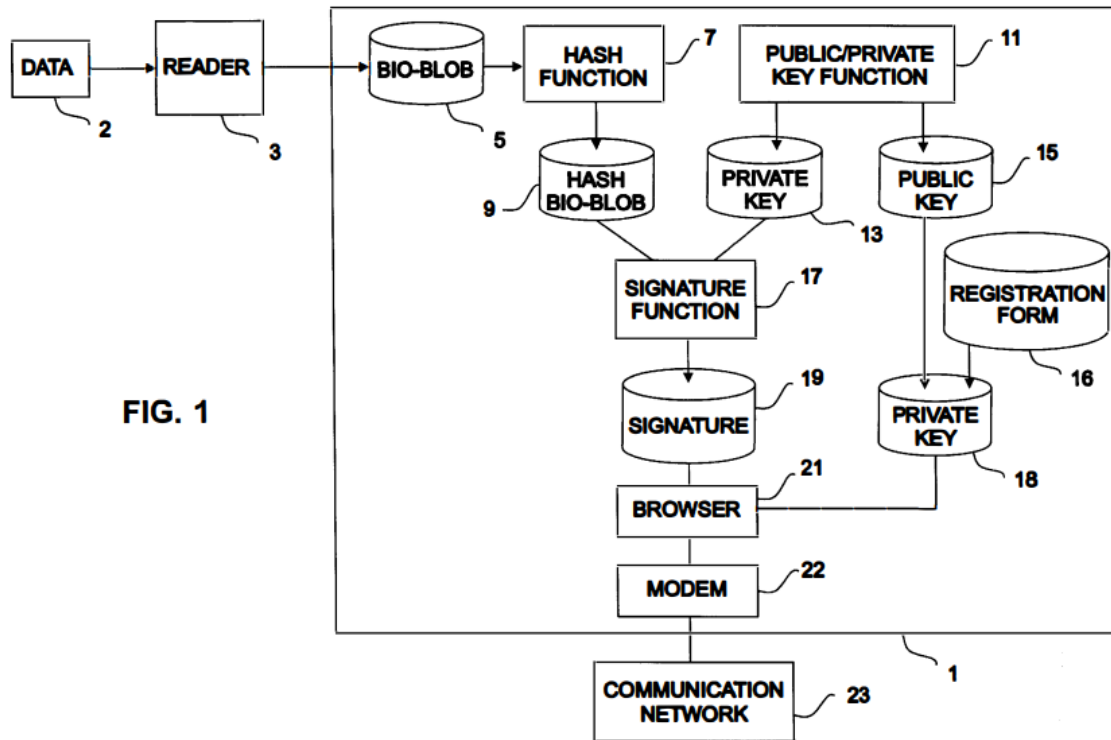


Figure 1, above, is a block diagram illustrating reader 3 connected to terminal 1 comprising, among other things, bio-blob data 5, hash function 7, hashed bio-blob 9, signature function 17, browser 21, and modem 22. *Id.* at 3:49–51, 4:54–56, 4:62–63, 5:12–17, 5:26–28, Fig. 1.

Data 2 containing bio-blob data 5 produced by the service provider is inserted into reader 3 and bio-blob data 5 is transferred to terminal 1. *Id.* at 4:56–60. Terminal 1 may be, for example, a computer workstation. *Id.* at 4:54–55. Data 2 is preferably a smart card and reader 3 is preferably a smart card reader. *Id.* at 4:54–61.

Hash function 7 receives bio-blob data 5 and calculates hashed bio-blob 9. *Id.* at 4:62–63. Hashed bio-blob 9 and private key 13 are received by

signature function 17. *Id.* at 5:13–14. Signature function 17 signs hashed bio-blob 9 by encrypting it with private key 13 to generate signature 19. *Id.* at 5:14–16. Public key 15 is combined with registration form 16 to create message 18. *Id.* at 5:24–25. Signature function 17 and message 18 are formatted by browser function 21 for transmission across communication network 23 via modem 22. *Id.* at 5:25–28. Communication network 23 allows communication between and among terminal 1, certificate authority 25, and receiving terminal 83. *Id.* at 5:35–38.

2. *Independent Claim 1*

a) *Petitioner’s Reasons to Combine are Insufficient*

The Supreme Court has explained that an obviousness analysis should “determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418. Similarly, the Federal Circuit has made clear that “[t]he factual inquiry whether to combine references must be thorough and searching” (*In re Nuvasive, Inc.*, 842 F.3d 1376, 1381 (Fed. Cir. 2016) (quoting *In re Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002)), and that an obviousness determination “cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness” (*In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)). *See KSR*, 550 U.S. at 418 (quoting *Kahn*, 441 F.3d at 988); *see also Lee*, 277 F.3d at 1342, 1345 (“The board cannot rely on conclusory statements when dealing with particular combinations of prior art and specific claims, but must set forth the rationale on which it relies.”).

Petitioner asserts that a person having ordinary skill in the art “would have been motivated to implement *Gullman* such that its token includes the owner’s biometric input.” Pet. 33. Petitioner asserts that its proposed

modification “would increase system security by enabling the host to perform its own confirmatory biometric comparison.” *Id.* Dr. Neuman testifies that a person having ordinary skill in the art “would have recognized that the security of *Gullman*’s system could therefore be improved by including the owner’s biometric input within the encrypted token.” Ex. 1003 ¶ 81.

Relying on the testimony of Dr. Russ, Patent Owner argues that Petitioner “has not explained how or why a PHOSITA would modify the simple system of *Gullman*—designed to be ‘reliable’ and provide transmission security that is ‘convenient, secure and useful’ on existing systems (Ex-1004, 6:46–56)—with the complex encryption process from *Padgett* that requires hashing and ‘dehashing’ to ‘recover’ the bio-blob 5.” Prelim. Resp. 40 (citing Ex. 2001 ¶¶ 116–117). Dr. Russ testifies that a person having ordinary skill in the art would not have been motivated to make Petitioner’s proposed modification “because it would have imparted considerable complexity to *Gullman*’s system, which teaches that a ‘significant advantage’ of its system is that it is more ‘convenient.’” Ex. 2001 ¶ 117 (citing Ex. 1004, 6:46–56).

Dr. Russ also testifies as follows:

A PHOSITA would recognize that the use of a biometric correlation as part of the token is a fundamental feature of *Gullman*—it eliminates the need for (1) a biometric template to be transmitted to the host, (2) the biometric input to be encrypted as part of the token and transmitted to the host, (3) the host to store the template, and (4) the host to perform a biometric comparison to authorize the user. That makes the system more secure, because it eliminates the risk of the biometric template and input from being stolen during transmission or while they are stored on the host. It also eliminates the major security risk of aggregating all biometric templates at a central location (host 10)

or transmitting all of the biometric inputs to a central location. Gullman's system is instead purposefully designed so that the host uses the correlation factor to determine whether the user was properly authenticated by the biometric security device.

Id. ¶ 119. Dr. Russ testifies that another benefit of Gullman's system is that "the amount of data that must be transmitted to the host" is reduced. *Id.*

¶ 122.

Based on the record before us, we find Petitioner's argument unavailing. Rather, we agree with Patent Owner and we credit Dr. Russ's testimony as Dr. Russ's testimony is consistent with the evidence of record.

Petitioner's assertion that its proposed modification "would increase system security" (Pet. 33), and Dr. Neuman's testimony that a person of ordinary skill in the art "would have recognized that the security in *Gullman's* system could . . . be improved by including the owner's biometric input within the encrypted token" (Ex. 1003 ¶ 81) are conclusory and unpersuasive on this record. Petitioner does not address the full teachings of Gullman. Contrary to Petitioner's assertion (Pet. 33; Ex. 1003 ¶ 81) and consistent with Patent Owner's position and Dr. Russ's testimony that Gullman's system eliminates the risk of the biometric template and input from being stolen during transmission (Ex. 2001 ¶ 119), Gullman describes its system as "secure," providing "secure identification," and, importantly, as providing "[t]ransmission security." Ex. 1004, 6:46–56.

Petitioner also does not address Gullman's teaching that its system provides "significant advantages" over known, more complex systems, which might have led an ordinarily skilled artisan away from using Padgett's more complicated hashing process. *Id.* In particular, Gullman states the following:

The method and apparatus of the present invention have significant advantages over known security systems. Reliable and secure identification is provided which eliminates the need for the user to memorize a code or carry a printed memorandum of the code. Transmission security is provided which is convenient, secure and useful on existing access devices of host systems in current use. In particular, the method and apparatus obviate the need for specially-designed hardware additions or modifications to existing access devices.

Id.

Gullman's teaching that a "significant" advantage of its system is that it is "convenient" (*id.*) is consistent with Patent Owner's position and Dr. Russ's testimony that a person having ordinary skill in the art would not have been motivated to make Petitioner's proposed modification because of the added complexity. Petitioner does not address the complexities of Padgett including performing a hashing function, generating public and private keys, generating a signature, creating a message, and transmitting the message and signature. Ex. 1006, 4:62–5:28. Petitioner provides the testimony of Dr. Neuman that multiple proposed modifications to Gullman's system would have been needed including that an encrypted token would have needed to include the owner's biometric input "rather than (or in addition to) the correlation factor," the security apparatus would have needed to "transfer the owner's biometric information to the host," and the host would have needed to "retrieve the template." Ex. 1003 ¶¶ 81–82. Petitioner does not indicate or provide evidence supporting that the proposed modifications would have been made without introducing complexities, or that an ordinarily skilled artisan would still have had reason to combine Gullman with Padgett despite the added complexities. We credit Dr. Russ's testimony that the changes "would have imparted considerable complexity to

Gullman's system" (Ex. 2001 ¶ 117) as consistent with the evidence of record including the teachings of Padgett.

Furthermore, we find that Dr. Russ's testimony that the use of a biometric correlation, rather than biometric input, as part of the token is a fundamental feature of Gullman (*id.* ¶ 119) is consistent with Gullman's teachings. Importantly, Gullman describes use of the correlation factor throughout. *See, e.g.*, Ex. 1004, 2:55–59 (describing that the "verification algorithm" derives "a token output"), 3:39–48 (describing that the security apparatus derives "a correlation factor"), 4:29–31 (describing that the host "verifies the identification [of the user] based on the correlation factor"), 5:15–19 (describing applying "an encryption algorithm to the time of day from real time clock 25, the fixed code and a biometric correlation factor, generating an encrypted security token"), 6:12–17 (describing that "the biometric input is compared to one or more stored templates" and a "correlation factor is calculated for each template"), 6:38–39 (describing that the host "decrypts or decodes the token to derive the fixed code and correlation factor"). Petitioner has not sufficiently shown why one of ordinary skill would modify this fundamental feature of Gullman.

In summary, we are not persuaded by Petitioner assertion that a person having ordinary skill in the art would have modified Gullman's system because Petitioner's proposed modification "would [have] increase[d] system security." Pet. 33. Petitioner does not address that Gullman describes its system as "convenient" and already "secure." Ex. 1004, 6:46–55. Petitioner also does not address that, in contrast, Padgett's system involves complexities, such as performing a hashing function, generating public and private keys, generating a signature, creating a message, and transmitting the message and signature. Ex. 1006, 4:62–5:28.

Petitioner's assertion that its proposed modification "would [have] increase[d] system security" (Pet. 33) is conclusory, attorney argument that does not take into account the full teachings of Gullman and Padgett.

Petitioner also asserts that a person having ordinary skill in the art would have been motivated to make its proposed modification based on an express teaching in Padgett and a "similar 'trust' dynamic" in Gullman. Pet. 34. More specifically, Petitioner asserts the following:

As described above, *Padgett* teaches that "simply verifying that the sender has a valid certificate 71 from a reputable certificate authority 25 is sufficient" for many transactions but notes that "[a]n additional level of security can be obtained by recovering the bio-blob 5 from the certificate 71 and comparing it with the bio-blob . . . stored in the registered bio-blob database 39 during the registration process." *Padgett* (Ex. 1006), 7:58–8:10. In other words, many recipients will be satisfied that the sender has previously registered, but some will demand the additional assurance of confirming that the sender is authentic by performing a biometric comparison on the recipient side.

Pet. 34. Petitioner asserts that a "similar 'trust' dynamic exists in Gullman's teachings" because the host is asked "to trust that the security apparatus performed a proper biometric comparison and correctly authenticated the owner." *Id.* (citing Ex. 1003 ¶ 80).

Dr. Neuman testifies as follows:

Gullman teaches a similar trust dynamic in that *Gullman's* embodiments which include only a correlation factor in the token, rather than the biometric input itself, require the host to trust that the security apparatus performed a proper biometric comparison and correctly authenticated the owner. In such an embodiment, the host computer would be unable to independently verify that the biometric information was correct. If the security apparatus was compromised, it could lie to the host and certify that a match was confirmed even when that was not the case.

Ex. 1003 ¶ 80.

Patent Owner asserts that “[t]he ‘trust dynamic’ of Gullman and Padgett are not ‘similar,’ they are complete opposites.” Prelim. Resp. 41 (citing Ex. 2001 ¶ 121). Patent Owner asserts that Gullman’s design “provides numerous benefits over using a biometric input in the token.” *Id.* (citing Ex. 2001 ¶ 122). Relying on the testimony of Dr. Russ, Patent Owner also asserts that a person having ordinary skill in the art would have understood “that Padgett took the exact opposite approach to the one purposefully selected by Gullman.” *Id.* at 42 (quoting Ex. 2001 ¶ 123).

Based on the record before us, we find Petitioner’s argument that a Padgett’s teachings apply to Gullman because a “similar ‘trust’ dynamic exists in Gullman’s teachings” is misplaced. Rather, we agree with Patent Owner and we credit Dr. Russ’s testimony over Dr. Neuman’s testimony as Dr. Russ’s testimony is consistent with the evidence of record.

Dr. Neuman’s testimony that Gullman teaches a “similar trust dynamic” to that of Padgett (Ex. 1003 ¶ 80) is not consistent with the teachings of Gullman or Padgett. Padgett teaches obtaining “[a]n additional level of security” by certificate authority 25 performing a comparison of extracted bio-blob 5. Ex. 1006, 7:58–8:10. In contrast, Gullman’s host trusts the security apparatus to perform the biometric comparison and correctly authenticate the owner. *See, e.g.*, Ex. 1004, 4:29–31 (describing that host 10 “verifies the identification based on the correlation factor”), 6:38–42 (describing that the host “decrypts or decodes the token to derive the fixed code and correlation factor” and access is permitted if “the correlation factor is above the threshold level”). Dr. Neuman’s testimony does not include citations to supporting teachings in Gullman. Ex. 1003 ¶ 80. Dr. Neuman’s further testimony that Gullman’s security apparatus “could lie to the host”

(*id.*) pertains to an undefined possibility and does not substitute for an actual teaching in Gullman, in which, as discussed above, the security apparatus is trusted for authentication.

In summary, we are not persuaded by the Petition that a person having ordinary skill in the art would have been motivated based on the express teaching in Padgett and a “similar ‘trust’ dynamic” in Gullman. Pet. 34. Instead, we are persuaded that in Gullman, the host trusts the security apparatus, which is different than and not similar to Padgett’s teachings.

We, therefore, determine Petitioner has not shown sufficiently that a person having ordinary skill in the art would have combined the teachings of Gullman, Laczko, and Padgett in the manner described in the Petition.

b) Conclusion—Obviousness of Claim 1 over Gullman, Laczko, and Padgett

After consideration of the contentions and the evidence of record, we determine that Petitioner has not sufficiently articulated reasoning with a rational underpinning as to why one of ordinary skill in the art would have combined the teachings of Gullman, Laczko, and Padgett in the manner described in the Petition. Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claim 1 is unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman, Laczko, and Padgett.

3. Independent Claims 4, 5, 7, and 10

Petitioner’s reasons to combine apply to all independent claims. Pet. 30–36. Petitioner does not supplement its reasons to combine the assert art for any of independent claims 4, 5, 7, and 10. *See, e.g., id.* at 38–39.

For the reasons given for claim 1, we determine that Petitioner has not offered sufficient articulated reasoning with a rational underpinning as to

why one of ordinary skill in the art would have combined the teachings of Gullman, Laczko, and Padgett in the manner described in the Petition. Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 4, 5, 7, and 10 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman, Laczko, and Padgett.

4. Dependent Claims 2, 8, 13, and 14

Claim 2 depends directly from claim 1. Claim 8 depends directly from claim 7. Claim 13 depends directly from claim 4 and claim 14 depends directly from claim 5. Petitioner's arguments and evidence for dependent claims 2, 8, 13, and 14 do not remedy the deficiencies discussed with respect to claims 1, 4, 5, and 7.

Accordingly, we conclude that Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 2, 8, 13, and 14 are unpatentable under 35 U.S.C. § 103 as obvious over the combination of Gullman, Laczko, and Padgett.

IV. CONCLUSION

We have reviewed the Petition and Preliminary Response, and have considered all of the evidence and arguments presented by Petitioner and Patent Owner. For the foregoing reasons, we conclude that the information presented in the Petition does not establish a reasonable likelihood that Petitioner would prevail in showing that the challenged claims of the '895 patent are unpatentable.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied, and no trial is instituted.

IPR2022-00172
Patent 8,489,895 B2

For PETITIONER:

Adam P. Seitz
Paul R. Hart
ERISE IP, P.A.
Adam.Seitz@eriseip.com
Paul.Hart@eriseip.com
PTAB@eriseip.com

For PATENT OWNER:

Stephen D. Zinda
James H. Hall
David Cabello
CABELLO HALL ZINDA, PLLC
stephen@chzfirm.com
james@chzfirm.com
david@chzfirm.com