

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

CPC PATENT TECHNOLOGIES PTY, LTD.,
Patent Owner.

IPR2022-00602
Patent 9,665,705 B2

Before SCOTT A. DANIELS, BARRY L. GROSSMAN, and
AMBER L. HAGY, *Administrative Patent Judges*.

GROSSMAN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

A. Background and Summary

Apple Inc. (“Petitioner” or “Apple”) filed a Petition for *inter partes* review of claims 1, 4, 6, 10–12, and 14–17 (collectively, the “challenged claims”) of U.S. Patent No. 9,655,705 B2 (Ex. 1001, “the ’705 patent”). Paper 1 (“Pet.”). CPC Patent Technologies PTY, Ltd. (“Patent Owner” or “CPC”) timely filed a Preliminary Response to the Petition. Paper 7 (“Prelim. Resp.”). With our authorization, Petitioner filed a Preliminary Reply (Paper 8 (“Prelim. Reply”)) addressing the issue of discretionary denial raised in the Preliminary Response and Patent Owner filed a Prelim. Sur-Reply (Paper 9 (“Prelim. Sur-Reply”)).

We concluded that Petitioner satisfied the burden, under 35 U.S.C. § 314(a), to show that there was a reasonable likelihood that Petitioner would prevail with respect to at least one of the challenged claims. Accordingly, on behalf of the Director (37 C.F.R. § 42.4(a)), and in accordance with *SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1353 (2018), we instituted an *inter partes* review of all the challenged claims, on all the asserted grounds. Paper 11 (“Dec. Inst.”).

Patent Owner filed a Response. Paper 17 (“PO Resp.”). Petitioner filed a Reply. Paper 20 (“Reply”). Patent Owner filed a Sur-reply. Paper 26 (“Sur-reply”).

Petitioner submitted eighty exhibits. *See* Exs. 1001–1091¹ (some consecutive exhibit numbers were *not* used; *e.g.*, there are no exhibits

¹ Exhibit 1091 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. *See* PTAB Consolidated Trial Practice Guide, 84 (Nov. 2019 (“TPG”)) (“Demonstrative exhibits used at the final hearing are aids to oral argument and not evidence”).

numbered 1056–1064); *see also* Paper 28 (Petitioner’s Updated Exhibit List stating that Exhibit numbers 1056–1064 were “Intentionally left blank.”). Petitioner relies on the Declaration testimony of Andrew Sears, Ph.D. *See* Exs. 1003, 1090.

Patent Owner submitted sixteen exhibits. *See* Exs. 2001–2016²; *see also* Paper 29 (Patent Owner’s Updated Exhibit List). Patent Owner relies on the Declaration testimony of William C. Easttom III, D. Sc., Ph.D. *See* Exs. 2013, 2014.

A hearing was held June 29, 2023. (Paper 30) (“Transcript or “Tr.”).

We have jurisdiction under 35 U.S.C. § 6. We enter this Final Written Decision pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

Petitioner has the burden of proving unpatentability of a claim by a preponderance of the evidence. 35 U.S.C. § 316(e).

Based on the findings and conclusions below, we determine that Petitioner has proven that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

B. Real Parties-in-Interest

Apple identifies itself as the sole real party-in-interest. Pet. 62.

CPC also identifies itself as the sole real party-in-interest. Paper 4, 2.

C. Related Matters

Petitioner and Patent Owner each identify the following two district court proceedings as related matters: (1) *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, Case No. 6:21-cv-00165-ADA (W.D. Tex.); and (2) *CPC Patent Technologies Pty Ltd. v. HMD Global Oy*, Case No. 6:21-cv-00166-ADA (W.D. Tex.) (the “HMD W.D. Texas case”). Pet. 62; Paper 4, 2.

² Exhibit 2016 is a demonstrative exhibit used at the final hearing. It is not an evidentiary exhibit. *See id.*

The first listed case, between the same parties involved in this *inter partes* review proceeding, however, has been transferred to the Northern District of California. *See In re Apple Inc.*, 2022 WL 1196768 (Fed. Cir. Apr. 22, 2022); *see also* Ex. 3002 (Text Order granting Motion to Change Venue). The case is now styled *CPC Patent Technologies Pty Ltd. v. Apple Inc.*, No. 5:22-cv-02553 (N.D. Cal.) (the “Apple N.D. California case”). *See* Ex. 3003 (PACER Docket for the transferred case); Prelim. Resp. 1, fn 1 (Patent Owner acknowledging the transfer from the Western District of Texas to the Northern District of California).

Petitioner and Patent Owner also each identify the following two pending *inter partes* review proceedings as related matters: (1) IPR2022-00600, challenging claims in Patent 8,620,039; and (2) IPR2022-00601, challenging claims in Patent 9,269,208, which is the “parent” of the ’705 patent. *See* Ex. 1001, code (63). A final written decision in the 00600 IPR is due October 17, 2023. A final written decision in the 00601 IPR is being issued simultaneously with this Decision in the case before us.

D. The ’705 Patent

We make the following findings concerning the disclosure of the ’705 patent.

The ’705 patent discloses a system “for providing secure access to a controlled item.” Ex. 1001, Abstr. The “controlled item” can be, for example, the locking mechanism of a door or an electronic lock on a personal computer. *Id.* at 1:43–46.³ The system uses a database of “biometric signatures” (*id.* at 2:32), such as a fingerprint (*id.* at 7:36) for determining authorized access.

³ Citations are to column:line[s] of the ’705 patent.

Figure 2 from the '705 patent is reproduced below.

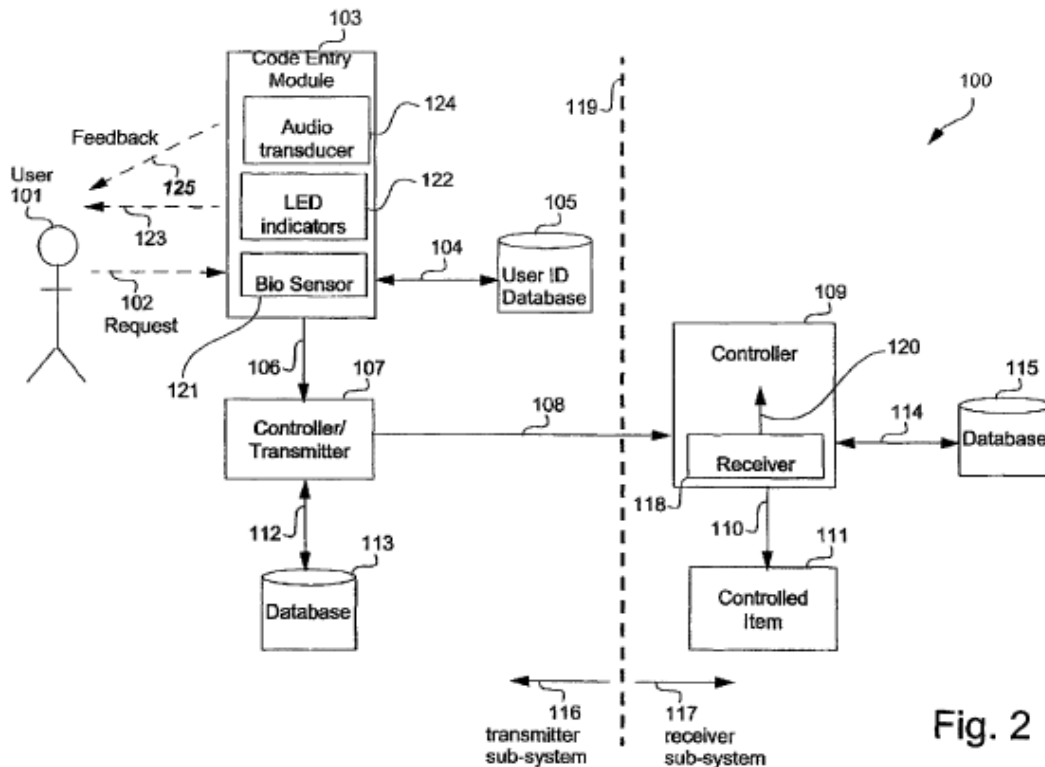


Fig. 2

Figure 2 is a functional block diagram of an arrangement for providing secure access according to the system disclosed in the '705 patent. Ex. 1001, 5:18–19.

As described in the written description of the '705 patent, and as illustrated generally in Figure 2, user 101 makes a request to code entry module 103. *Id.* at 5:56–57. Code entry module 103 includes biometric sensor 121. *Id.* at 5:57–58. If biometric sensor 121 is a fingerprint sensor, for example, then the request “typically takes the form of a thumb press” on a sensor panel (not shown) on code entry module 103. *Id.* at 5:60–63. “Other physical attributes that can be used to provide biometric signals include voice, retinal or iris pattern, face pattern, [and] palm configuration.” *Id.* at 1:30–32; *see also id.* at 16:45–49 (claim 4 stating “the biometric sensor

is responsive to one of voice, retinal pattern, iris pattern, face pattern, and palm configuration”).

Code entry module 103 then “interrogates” an authorized user identity database 105, which contains “biometric signatures” for authorized users, to determine if user 101 is an authorized user. Ex. 1001, 5:64–6:2. If user 101 is an authorized user, code entry module 103 sends a signal to “controller/transmitter” 107. *Id.* at 6:2–4. Database 105 is prepared by an “administrator.” *Id.* at 10:38–42 (“The first user of the code entry module 103 . . . is automatically categorised⁴ as an administrator.”).

The disclosed system and method compare biometric input “*signal*” 102 to database 105 of authorized biometric “*signatures*” to determine if user 101 is an authorized user. *Id.* at 5:65–6:2 (“Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 [producing a thumbprint] then the user database 105 contains biometric signatures [*i.e.*, thumbprints] for authorised users against which the request 102 can be authenticated.”). If user 101 is an authorized user, code entry module 103 sends a signal to “controller/transmitter” 107 allowing access to the controlled item. *Id.* at 6:2–10.

When biometric sensor 121 is a fingerprint sensor,⁵ the biometric signatures stored in database 105 are not limited to a single fingerprint. The ’705 patent also discloses that, if so programed by an administrator, code

⁴ The Specification uses the British spelling, which we also use when quoting the Specification.

⁵ See Ex. 1001, 10:35 – 38 (“Although the present description refers to ‘Users’, in fact it is ‘fingers’ which are the operative entities in system operation *when the biometric sensor 121 (see FIG. 2) is a fingerprint sensor.*”) (emphasis added). Thus, it is clear that biometric sensor 121 is *not* limited to a fingerprint sensor.

entry module 103 may be activated by providing a succession of finger presses to biometric sensor 121 included in module 103. *Id.* at 10:56–58. If these successive presses are of the appropriate duration, the appropriate quantity, and are input within a predetermined time, controller 107 accepts the presses “as potential control information,” or a biometric signal, and checks the input information against a stored set of “legal [authorized] control signals,” or the database of biometric signatures. *Id.* at 10:59–67. “In one arrangement, the control information is encoded by *either or both* (a) the number of finger presses and (b) the relative duration of the finger presses.” *Id.* at 10:60–63 (emphasis added).

An example of this type of “control information” or “legal control signal” is “dit, dit, dit, dah,” where “dit” is a finger press of one second’s duration . . . and “dah” is a finger press of two second’s duration.”⁶
Id. at 11:1–7.

⁶ We have not been directed to any persuasive evidence, and have found none on our own review of the evidence, which establishes why the Specification refers to the number and duration of finger presses as “control information” and “legal control signals,” rather than a “biometric signal” and a “database” of “biometric signatures,” respectively, which are the terms used throughout the Specification for the input signal and the database of authorized users.

The Specification is required to include “a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art . . . to make and use the same.” 35 U.S.C. § 112(a). Neither we nor the parties, however, have jurisdiction in this *inter partes* review proceeding to address this enablement issue. *See id.* at § 311(b) (“A petitioner in an *inter partes* review may request to cancel as unpatentable 1 or more claims of a patent only on a ground that could be raised under section 102 or 103 and only on the basis of prior art consisting of patents or printed publications.”).

If user 101 is an authorized user based on the inputs to code entry module 103, controller/transmitter 107 then sends “an access signal,” based on a “rolling code,” to controller 109. Ex. 1001, 6:2–9. According to the written description, “[t]he rolling code protocol offers non-replay encrypted communication.” *Id.* at 6:9–10. Other secure codes, such as “the Bluetooth™ protocol, or the Wi Fi™ protocols” also can be used. *Id.* at 6:32–38.

If controller 109 determines that the rolling code received is “legitimate,” then controller 109 sends a command to “controlled item 111,” which, for example “can be a door locking mechanism on a secure door, or an electronic key +circuit in a personal computer” that is to be accessed by user 101. *Id.* at 6:11–20.

Code entry module 103 also incorporates at least one mechanism for providing feedback to user 101. *Id.* at 6:24–25. This mechanism can, for example, take the form of “one or more Light Emitting Diodes (LEDs) 122,” and/or audio transducer 124, which provide visual or audio feedback to the user. *Id.* at 6:25–31.

In Figure 2, “sub-system 116,” shown on the left of vertical dashed line 119, communicates with “sub-system 117,” shown on the right of dashed line 119, “via the wireless communication channel” used by access signal 108 between controller/transmitter 107 and controller/receiver 109. *Id.* at 6:61–67. As disclosed in the ’705 patent, “[a]lthough typically the communication channel uses a wireless transmission medium, there are instances where the channel used by the access signal 108 can use a wired medium.” *Id.* at 7:9–14.

E. Illustrative Claim

Among the challenged claims, claims 1, 10, 11, 14, 15, 16, and 17 are independent claims.

Independent claims 1 and 15 are directed to a “system for providing secure access to a controlled item.” Ex. 1001, 15:62–63; 18:39–40. These claims are identical except for claim 1 using the phrase “configured to,” whereas claim 15 uses the phrase “capable of.” For example, claim 1 includes “a biometric sensor *configured to receive* a biometric signal” (*id.* at 15:66–67 (emphasis added)), whereas claim 15 includes “a biometric sensor *capable of receiving* a biometric signal.” (*id.* at 18:43–44 (emphasis added)). This same distinction also applies to the claimed elements of “a transmitter sub-system controller,” “a transmitter,” and “a receiver sub-system controller.” *Compare id.* at 16:1–23 (claim 1) *with id.* at 18:45–67 (claim 15).

We discuss below in Section II.C (Claim Construction) whether use of the phrase “capable of” rather than the phrase “configured to” is a distinction without a substantive difference.

Independent claims 10 and 16 are directed to a “transmitter sub-system for operating in a system for providing secure access to a controlled item.” *Id.* at 17:19–20; 19:1–2. The only distinction between claims 10 and 16 is the same “capable of”/“configured to” distinction discussed above for claims 1 and 15. *Compare id.* at 17:19–39 (claim 10) *with id.* at 19:1–20 (claim 16).

Independent claims 11 and 17 are directed to a “method for providing secure access to a controlled item.” *Id.* at 17:40–41. The only distinction between claims 11 and 17 is the same “capable of”/“configured to” distinction discussed above for claims 1 and 15. Again, the only distinction

between claims 11 and 17 is the same “capable of”/”configured to” distinction discussed above for claims 1 and 15. *Compare id.* at 17:40–67 (claim 11) *with id.* at 19:21–20:23 (claim 17).

Independent claim 14 is directed to a “non-transitory computer readable storage medium storing a computer program.” *Id.* at 18:18–19.

Independent claim 1 is illustrative and is reproduced below.

1. A system for providing secure access to a controlled item, the system comprising:
 - a memory comprising a database of biometric signatures;
 - a transmitter sub-system comprising:
 - a biometric sensor configured to receive a biometric signal;
 - a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute;
 - and
 - a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and
 - a receiver sub-system comprising:
 - a receiver sub-system controller configured to:
 - receive the transmitted secure access signal; and
 - provide conditional access to the controlled item dependent upon said information;
 - wherein the transmitter sub-system controller is further configured to:
 - receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;
 - map said series into an instruction; and
 - populate the data base according to the instruction,
- wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

Ex. 1001, 15:62–16:23.⁷

F. Prior Art and Asserted Grounds

Petitioner asserts that the challenged claims are unpatentable on the following ground:

Claim(s) Challenged	35 U.S.C. §⁸	Reference(s)/Basis
1, 4, 6, 10–12, 14–17	103(a)	Mathiassen, ⁹ McKeeth, ¹⁰ Anderson ¹¹

Petitioner also relies on the declaration testimony of Andrew Sears, Ph.D. *See* Ex. 1003.¹²

⁷ Petitioner provides a Claim Listing Appendix as part of the Petition. Pet. 64–69. This Appendix includes all the challenged claims identified by individual clause, such as, for claim 1, labeling the clauses 1(a), 1(b), 1(b)(1), etc. Petitioner refers to these clause labels in its analysis.

⁸ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 296–07 (2011), took effect on September 16, 2011. The changes to 35 U.S.C. §§ 102 and 103 in the AIA do not apply to any patent application filed before March 16, 2013. Because the application for the patent at issue in this proceeding has an effective filing date before March 16, 2013, we refer to the pre-AIA version of the statute.

⁹ Mathiassen et al, US 2004/0123113 A1, published June 24, 2004 (Ex. 1004, “Mathiassen”).

¹⁰ McKeeth, US 6,766,456 B1, issued July 20, 2004 (Ex. 1005, “McKeeth”).

¹¹ Anderson, US 6,509,847 B1, issued Jan. 21, 2003 (Ex. 1006, “Anderson”).

¹² Exhibit 1003 is a 238-page declaration from Dr. Sears, including its Appendix A, which is a detailed mapping of the disclosures of the three applied references to the challenged claims. Dr. Sears currently is a Professor and Dean of the College of Information Sciences and Technology at The Pennsylvania State University. Ex. 1003 ¶ 5. Dr. Sears earned a Bachelor of Science degree in Computer Science, and a Ph.D. degree, also in Computer Science. *Id.* ¶ 6. He has held various positions in academia, including serving as the Interim Chief Information Security Officer at Penn State. *Id.* ¶¶ 7, 8. He has authored or edited a number of computer-related publications and held leadership positions in several computer industry organizations. *Id.* ¶¶ 10–12.

II. ANALYSIS

A. Obviousness

Section 103 forbids issuance of a patent when “the differences between the subject matter sought to be patented 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 available, evidence such as commercial success, long felt but unsolved needs, and failure of others.¹³ *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966); *see KSR*, 550 U.S. at 407 (“While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.”). The Court in *Graham* explained that these factual inquiries promote “uniformity and definiteness,” for “[w]hat is obvious is not a question upon which there is likely to be uniformity of thought in every given factual context.” *Graham*, 383 U.S. at 18.

The Supreme Court made clear that we apply “an expansive and flexible approach” to the question of obviousness. *KSR*, 550 U.S. at 415. Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions.

¹³ Patent Owner does not direct us to any objective evidence of non-obviousness in its Preliminary Response.

Id. at 417. To support this conclusion, however, it is not enough to show merely that the prior art includes separate references covering each separate limitation in a challenged claim. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness additionally requires that a person of ordinary skill at the time of the invention “would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention.” *Id.*

In determining whether there would have been a motivation to combine prior art references to arrive at the claimed invention, it is insufficient to simply conclude the combination would have been obvious without identifying any reason *why* a person of skill in the art would have made the combination. *Metalcraft of Mayville, Inc. v. Toro Co.*, 848 F.3d 1358, 1366 (Fed. Cir. 2017).

Moreover, in determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985) (“It is elementary that the claimed invention must be considered as a whole in deciding the question of obviousness.”); *see also Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983) (“[T]he question under 35 U.S.C. § 103 is not whether the differences *themselves* would have been obvious. Consideration of differences, like each of the findings set forth in *Graham*, is but an aid in reaching the ultimate determination of whether the claimed invention *as a whole* would have been obvious.”).

As a factfinder, we also must be aware “of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.” *KSR*, 550 U.S. at 421.

Applying these general principles, we consider the evidence and arguments of the parties.

B. Level of Ordinary Skill in the Art

The level of skill in the art is “a prism or lens” through which we view the prior art and the claimed invention. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). “This reference point prevents . . . factfinders from using their own insight or, worse yet, hindsight, to gauge obviousness.” *Id.*

Factors pertinent to a determination of the level of ordinary skill in the art include: (1) educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of workers active in the field. *Env’t Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case. *Id.* Moreover, these factors are not exhaustive but are merely a guide to determining the level of ordinary skill in the art. *Daiichi Sankyo Co. v. Apotex, Inc.*, 501 F.3d 1254, 1256 (Fed. Cir. 2007). In determining a level of ordinary skill, we also may look to the prior art, which may reflect an appropriate skill level. *Okajima*, 261 F.3d at 1355.

“The *Graham* analysis includes a factual determination of the level of ordinary skill in the art. Without that information, a district court cannot

properly assess obviousness because the critical question is whether a claimed invention would have been obvious at the time it was made to one with ordinary skill in the art.” *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986); *see also Ruiz v. A.B. Chance*, 234 F.3d 654, 666 (Fed. Cir. 2000) (“The determination of the level of skill in the art is an integral part of the *Graham* analysis.”).

Neither party provides any persuasive evidence or argument concerning the factors identified above or any other factors relevant to determining the level of ordinary skill.

Petitioner asserts that a person of ordinary skill in the art would have had “at least a bachelor’s degree in computer engineering, computer science, electrical engineering, or a related field, with at least one year experience in the field of human-machine interfaces and device access security.” Pet. 4 (citing Ex. 1003 ¶¶ 31–35).¹⁴ Petitioner also states that “[a]dditional education or experience may substitute for the above requirements.” *Id.*

In forming an opinion on the level of ordinary skill applicable to this proceeding, Dr. Sears testifies that he considered various factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the education level of active workers in the field. Ex. 1003 ¶ 31. Dr. Sears also testifies that he “placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time.” *Id.* Dr. Sears opines that a person of ordinary skill

¹⁴ Petitioner cites this testimony as “Dec.” Pet. 4, fn 1. We will cite it, as we do all other evidence, by reference to its Exhibit number, which is Exhibit 1003.

would have had the education and experience adopted by Petitioner.

Id. at ¶ 32.

Patent Owner states it “does not dispute [Petitioner’s] characterization” of the level of ordinary skill in the art. *See* PO Resp. 5–6.

Based on the prior art, the sophistication of the technology at issue, and Dr. Sears’ Declaration testimony, we adopt, with minor modification, Petitioner’s undisputed definition of the level of ordinary skill. We determine that in this proceeding a person of ordinary skill would have had a bachelor’s degree in computer engineering, computer science, electrical engineering, or a related field, with one year of experience in the field of human-machine interfaces and device access security, or an equivalent balance of education and work experience. We have eliminated the open-ended phrase of “at least” in describing the education and experience of a person of ordinary skill. This open-ended description fails to provide the specificity necessary to define the level of ordinary skill.

C. Claim Construction

We construe each claim “using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b).” 37 C.F.R. § 42.100(b) (2021). Under this standard, claim terms are generally given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (en banc) (“We have frequently stated that the words of a claim ‘are generally given their ordinary and customary meaning.’” (citations omitted)).

Petitioner states that in the related district court litigation between the parties, the Western District of Texas court entered a Claim Construction

Order on February 10, 2022. (Ex. 1077). Pet. 5. Petitioner also states “the Parties agreed to certain constructions in a Joint Claim Construction Statement” in the Western District of Texas litigation (Ex. 1074). *Id.* Petitioner then proposes that “[f]or purposes of this IPR, Apple applies the District Court’s constructions from the *Apple* litigation [Ex. 1077] and constructions agreed to by the Parties (Ex. 1074)^[15] that are not otherwise plain and ordinary meaning.” *Id.*

Petitioner also highlights specific constructions for the claim terms “database,” “conditional access,” “biometric signal,” and “accessibility attribute” from Exhibits 1074 and 1077. Pet. 6.

Patent Owner proposes “constructions” (1) for the term “accessibility attribute” (PO Resp. 6–7); (2) the phrase requiring a series of entries of the biometric signal “characterised according to at least one of the number of said entries and a duration of each said entry” (*id.* at 7–11); and (3) the “populate” the database limitation concerning enrolling or authorizing new users (*id.* at 11–12).

Patent Owner also provided its views on the differences in claim scope between the term “configured to” and the term “capable of” as used in the challenged claims. *Id.* at 12–14. Petitioner also addresses this topic. Reply 26.

“[W]e need only construe terms ‘that are in controversy, and only to the extent necessary to resolve the controversy.’” *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Ltd.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795,

¹⁵ The cited Exhibits 1074 and 1077 are from the case *prior to* its transfer from the Western District of Texas to the Northern District of California.

803 (Fed. Cir. 1999)). Here, we determine the claim terms that need specific construction are the three terms proposed by Patent Owner for specific construction. Accordingly, we construe these terms below.

1. General Claim Construction Principles

“It is a ‘bedrock principle’ of patent law that ‘the claims of a patent define the invention to which the patentee is entitled the right to exclude.’” *Phillips*, 415 F.3d at 1312 (citations omitted). “[T]here is no magic formula or catechism for conducting claim construction.” *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 801, 809 (Fed. Cir. 2021) (quoting *Phillips*, 415 F.3d at 1324). Fortunately, however, there is substantial judicial guidance.

Claim construction requires determining how a skilled artisan would understand a claim term “in the context of the entire patent, including the specification.” *Grace Instrument Indus., LLC v. Chandler Instruments Co., LLC*, 57 F.4th 1001, 1008 (Fed. Cir. 2023) (quoting *Phillips*, 415 F.3d at 1313. *Id.* (citation omitted). “[C]laims must be read in view of the specification, of which they are a part.” *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 978 (Fed. Cir. 1995) (en banc)). The Specification, or more precisely, the written description, is the “single best guide to the meaning of a disputed term.” *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)), and “is, thus, the primary basis for construing the claims.” *Id.* (citation omitted). Although claim terms are interpreted in the context of the entire patent, it is improper to import limitations from the Specification into the claims. *Phillips*, 415 F.3d at 1323. Thus, we are careful not to cross that “fine line” that exists between properly construing a claim in light of the specification and improperly importing into the claim a limitation from the specification.” *Comark Commc 'ns., Inc. v. Harris Corp.*, 156 F.3d 1182, 1186 (Fed. Cir.

1998) (“We recognize that there is sometimes a fine line between reading a claim in light of the specification, and reading a limitation into the claim from the specification.”).

While certain terms may be at the center of the claim construction debate, the context of the surrounding words of the claim also must be considered in determining the ordinary and customary meaning of those terms. *ACTV, Inc. v. Walt Disney Co.*, 346 F.3d 1082, 1088 (Fed. Cir. 2003).

We also consider the patent’s prosecution history. *Phillips*, 415 F.3d at 1317.

In construing the claims, we may also look to available “extrinsic evidence concerning relevant scientific principles, the meaning of technical terms, and the state of the art.” *Phillips*, 415 F.3d at 1314 (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004)).

2. “Accessibility Attribute”

In our Decision to Institute this proceeding, we adopted, for purposes of that Decision, Petitioner’s unopposed asserted claim construction for “accessibility attribute,” which was an “attribute that establishes whether and under which conditions access to the controlled item should be granted.” Dec. Inst. 13 (citing Pet. 6 (citing the Texas District Court’s claim construction, Exs. 1074, 1077)). We note here that the District Court included the phrase “to a user” at the end of the construed term, which Petitioner did *not* include. The complete construction by the District Court is an “attribute that establishes whether and under which conditions access to the controlled item should be granted *to a user.*” Ex. 1077, 2 (emphasis

added). The District Court did not cite any intrinsic or extrinsic evidence to support its construction.

In Patent Owner’s Response, Patent Owner acknowledges Petitioner’s proposed construction but asserts that “a mere binary decision to grant access to a device does not constitute an ‘accessibility attribute.’” PO Resp. 6–7; *see also* Ex. 2013 ¶ 45 (Patent Owner’s expert, Dr. Easttom,¹⁶ testimony that the construction of the term “accessibility attribute” in our Decision to Institute this proceeding “requires more than the binary determination of whether to grant access to a controlled item by virtue of the ‘under which conditions’ language.”). Patent Owner also asserts that Petitioner’s “position on the ‘accessibility attribute’ limitation is muddled at best.” PO Resp. 14. According to Patent Owner, Petitioner “and its expert appear to argue that ‘accessibility attribute’ *can* be a binary access decision.” *Id.* at 15 (citing Paper 1 [Pet.] at 18–20).

Thus, Patent Owner asserts what an “accessibility attribute” is not (it is not a “binary decision”), but fails to assert a construction of what an “accessibility attribute” is.

We do *not* understand Petitioner to be asserting a construction of the term “accessibility attribute” to mean simply a “binary decision” to grant or

¹⁶ Exhibit 2013 is a 36-page declaration from Dr. Easttom. Dr. Easttom earned a D.Sc. degree in Cyber Security, a Ph.D. degree in Technology, and three master’s degrees (one in Applied Computer Science, one in Education, and one in Systems Engineering). Ex. 2013 ¶ 7. Dr. Easttom testifies that he has 30 years of experience in the computer science industry including extensive experience with computer security, computer software, and computer networking; that he has authored 37 computer science books; that he has authored over 70 research papers; and that he is an inventor with 25 patents, including patents related to computer networking. His CV (Ex. 2014) provides details of his extensive experience and education.

not grant access to a locked structure or device. Nor did our Decision to Institute adopt such a “binary decision.” The construction asserted by Petitioner in this proceeding, and the construction adopted in our Decision to Institute this proceeding, requires “an attribute that establishes *whether and under which conditions* access to the controlled item should be granted.” Dec. Inst. 13 (citing Pet. 6 (citing the Texas District Court’s claim construction, Exs. 1074, 1077) (emphasis added)).

As we explain in our analysis below, to avoid any confusion of the meaning of “accessibility attribute,” we clarify the construction to add the phrase “if any” to modify the “conditions” that may, or may not, be imposed to allow access. Thus, we determine that an “accessibility attribute” is “an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted.” Based on the language of the claims and Specification, the “accessibility attribute” may include only an “access attribute,” which is “unconditional.” *See* Ex. 1001, 8:29–38 (stating “the accessibility attribute may comprise *one or more of* an access attribute (granting unconditional access),” a “duress attribute,” an “alert attribute,” and a “telemetry attribute”); *see also id.* at 16:34–44 (unchallenged claim 3 requiring an access attribute, a duress attribute, and an alert attribute).¹⁷

Notwithstanding Patent Owner’s Response that an “accessibility attribute” is not a “binary decision,” Petitioner asserts that “[t]he Parties agree to apply the District Court’s construction for the claimed ‘accessibility attribute.’” Reply 1. Petitioner also states, however, that Petitioner is relying on McKeeth for teaching two accessibility attributes (duress and

¹⁷ To avoid any confusion, we note that an “access attribute” is one specific example of the generic term “accessibility attribute.” Ex. 1001, 8:29–38.

alert) even though “the ’705 Patent’s independent claims only require outputting a single accessibility attribute.” *Id.* at 2.

Petitioner clarifies its position on the construction of “accessibility attribute” by further explaining Petitioner’s view that “the ’705 Patent describes “outputting an accessibility attribute that includes ‘access’ without any conditions, which satisfies the ‘under which conditions’ construction component.” Reply. 4.

We begin our claim construction analysis with the language used in the claims.

a) Claims

The term “accessibility attribute” appears directly or through dependency in all the challenged claims.

Independent claim 1 includes the following two clauses that refer to an “accessibility attribute”:

(1) “a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an *accessibility attribute*,” (Ex. 1001, 16:1–4)¹⁸; and

(2) “a transmitter configured to emit a secure access signal conveying information dependent upon said *accessibility attribute*” (*id.* at 16:5–7).

These two references merely establish that an “accessibility attribute” is an output access signal based on matching the biometric signal against the authorized user database of biometric signatures. *See id.* at 5:65–6:2 (“Thus for example if the request 102 is the thumb press on the biometric sensor panel 121 then the user database 105 contains biometric signatures for authorised [sic] users against which the request 102 can be authenticated.”).

¹⁸ All italicized emphasis of claim language has been added.

These clauses provide no further structure or function of the claimed “accessibility attribute.”

Claim 1 also includes a clause stating that “conditional access” to a user is “dependent upon” information in the “accessibility attribute.” *Id.* at 16:11–12. This clause does not require or state that there is, or is not, conditional access. It merely states that “conditional access,” if any, depends on what information is in the “accessibility attribute.” *See id.* at 16:5–7 (stating that the “information” in the “access signal” in claim 1 is “dependent upon” the “accessibility attribute”). Thus, based on the claim language in claim 1, the scope of the “accessibility attribute” is undefined. The only requirement is that it provide access for authorized users.

Claim 3 (not challenged, but still relevant to claim construction), dependent on claim 1, states that “the [authorized user] database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class.” Ex. 1001, 16:34–37 (emphasis added). Thus, consistent with Petitioner’s argument summarized above (*see* Reply 4–5), the system administrator may be the only authorized user in the database. Claim 3 also further defines the “accessibility attribute” as “comprising:

an access attribute if the biometric signal matches a member of the database of biometric signatures;

a duress attribute if the biometric signal matches a member of the database of biometric signatures *and said member belongs to the duress class*; and

an alert attribute if the biometric signal does not match a member of the database of biometric signatures.

Id. at 16:18–24 (emphases added).

In claim 3, the conditional “duress attribute” applies only if the user is a member of the “duress class” in the database of biometric signatures. There is, however, no requirement that any member of the “duress class” be in the database.

We recognize that the Federal Circuit has held that the plain and ordinary meaning of “at least one of” is “one or more,” but that when the phrase is used in a claim, the issue is what “at least one of” is used to modify. *See SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 886 (Fed. Cir. 2004). In *SuperGuide*, the court held that, when “[t]he phrase ‘at least one of’ precedes a series of categories of criteria, and the patentee used the term ‘and’ to separate the categories of criteria,” the phrase connotes a conjunctive list and requires selecting at least one value for each category. *Id.* For example, in *SuperGuide*, the claim phrase “storing at least one of a desired program start time, a desired program end time, a desired program service, and a desired program type” was interpreted as requiring storing at least one desired program start time, at least one desired program end time, and so forth. *Id.* at 884.

Courts have not, however, interpreted *SuperGuide* as setting forth a *per se* rule that the use of “at least one of” followed by “and” necessarily connotes a conjunctive list. *See Fujifilm Corp. v. Motorola Mobility LLC*, Case No. 12–CV–03587–WHO, 2015 WL 1265009, at *8 (N.D. Cal. Mar. 19, 2015) (summarizing cases and noting that “*SuperGuide* did not erect a universal rule of construction for all uses of ‘at least one of’ in all patents”). In particular, courts have found *SuperGuide* inapplicable when the listed items following “at least one of” are not categories containing many possible values. *See id.*; *see also TQ Delta, LLC v. Comcast Cable Commc’ns, LLC*, No. 1:15–CV–00611–RGA, 2016 WL 7013481, at *8 (D. Del. Nov. 30,

2016) (list following “at least one of” was of parameters to be selected from, not categories). The Board has also distinguished *SuperGuide* on this basis. See *Hewlett–Packard Co. v. MPHJ Tech. Invs., LLC*, Case IPR2013–00309, Paper 9, slip op. at 8 (PTAB Nov. 21, 2013); *Daifuku Co., Ltd. v. Murata Machinery, Ltd.*, Case IPR2015–00083, Paper 63, slip op. at 4–5 (PTAB May 3, 2016); *Apple, Inc. v. Evolved Wireless LLC*, No. IPR2016-01177, 2017 WL 6543970, at *4 (P.T.A.B. Dec. 20, 2017).

Relevant to our inquiry, therefore, is whether the items that follow “at least one of” in the challenged claims of the ’705 patent are categories that may have multiple values (such as in *SuperGuide*) or individual parameters having only one value. Here, we think it is clear that the accessibility attributes and the classes of users are individual parameters that apply to individual people.

As noted above, the first user of the disclosed and claimed invention “is automatically categorised as an administrator.” Ex. 1001, 10:38–42. This first user may be the only authorized user. Thus, the only database entry for this first user is a “system administrator class” entry that will generate only an “access attribute (granting *unconditional* access).” *Id.* at 8:29–30 (emphasis added). This is not unlikely because the claims are specifically limited to a “controlled item” that is either “a locking mechanism of a physical access structure,” or “an electronic lock on an electronic computing device.” See, e.g., *id.* at 16:21–23 (claim 1 stating “wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device”). A similar limitation is in each independent claim. The owner of an individual computing device may be the only authorized user of that device, thus having unconditional access as the “administrator.”

Claim 3 allows a database of only a first and only user, who is automatically the system administrator. Ex. 1001, 16:34–37 (“the database of biometric signatures comprises signatures in *at least one of* a system administrator class, a system user class, and a duress class” (emphasis added)). There may be no other individuals in the “system user class” or the “duress class.”

Claim 3 further limits claim 1 by stating the “accessibility attribute” in claim 1 comprises¹⁹ the three specific attributes stated in claim 3 – “an “access attribute;” “a duress attribute;” and “an alert attribute.” This listing in claim 3 establishes a presumption that these three requirements are *not* included in the claimed “accessibility attribute” in claim 1. *Phillips*, 415 F.3d at 1314–15 (“Differences among claims can also be a useful guide in understanding the meaning of particular claim terms. For example, the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.” (citations omitted)).²⁰

¹⁹ “[I]n general, a patent claim reciting an apparatus ‘comprising’ various components merely means that the apparatus ‘includ[es]’ but is not limited to ‘those components.’” *Rothschild Connected Devices Innovations, LLC v. Coca-Cola Co.*, 813 F. App’x 557, 562 (Fed. Cir. 2020) (nonprecedential) (citations omitted).

²⁰ We recognize that the Board “must base its decision on arguments that were advanced by a party, and to which the opposing party was given a chance to respond.” *Masimo Corp. v. Apple Inc.*, Nos. 2022-1631 *et al*, slip op. at 8 (Fed. Cir. Sep. 12, 2023 (nonprecedential)) (citing *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1381 (Fed. Cir. 2016)). The parties argued claim construction, but did not discuss specifically claim differentiation as part of their claim construction analysis. Petitioner argued, however, that the claims allowed for “administrator access as an exemplary access without conditions.” Reply 4–5. Patent Owner addressed this in its Sur-reply. Sur-

Based on the claim language, the doctrine of claim differentiation, and the analysis above, we determine that an “accessibility attribute,” as used in the challenged independent claims means that a user with a biometric signature in the database is given access to the controlled item. As used in the independent claims, there are no other conditions imposed.

Thus, based on the claim language, an “accessibility attribute” is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted.

b) Specification

Claims “must be read in view of the specification, of which they are a part.” *Phillips*, 415 F.3d at 1315 (citation omitted). “The specification “is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.” *Id.* (citation omitted). Thus, we turn to the Specification for additional guidance on the meaning of the claim term “accessibility attribute.”

The Specification states that the “accessibility attribute establishes whether and under which conditions access to the controlled item 111 should be granted to a user.” Ex. 1001, 8:26–28. This is the construction adopted in our Decision to Institute this proceeding.

reply 22. Our claim construction analysis, as stated in the text, follows controlling procedures from *Phillips*. The parties also were advised that: claim construction, in general, is an issue to be addressed at trial. Claim construction will be determined at the close of all the evidence and after any hearing. The parties are expected to assert all their claim construction arguments and evidence in the Petition, Patent Owner’s Response, or otherwise during trial, as permitted by our rules.

Dec. Inst. 14.

The Specification further states:

the accessibility attribute may comprise *one or more of an access attribute (granting unconditional access), a duress attribute (granting access but with activation of an alert tone to advise authorities of the duress situation), an alert attribute (sounding a chime indicating that an unauthorised, but not necessarily hostile, person is seeking access, and a telemetry attribute, which represents a communication channel for communicating state information for the transmitter sub-system to the receiver sub-system such as a “low battery” condition.*

Id. at 8:29–38 (emphases added). Thus, while four different accessibility attributes are disclosed (access attribute, duress attribute, alert attribute, and telemetry attribute), the Specification, consistent with the claims discussed above, states that the disclosed invention “may comprise *one or more of*” these four attributes. Ex. 1001, 8:29–30. The Specification also states that an “access attribute” grants “unconditional access.” *Id.* at 8:30.

The term “accessibility attribute” does not appear in the Specification after column 8 until it appears again in the claims.

Thus, based on the Specification, an “accessibility attribute” is an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted. The term “if any” is required because an “access attribute” grants “unconditional access” (*id.*) and it may be the only attribute included as an “accessibility attribute.” *See id.* at 8:29–38 (stating the accessibility attribute “may comprise one or more of” the four disclosed specific attributes).

c) Prosecution History

The parties have not directed us to any persuasive evidence from the proceedings leading to issuance of the ’705 patent to inform our construction of the term “accessibility attribute.”

d) Extrinsic Evidence

The parties do not direct us to any persuasive extrinsic evidence concerning the meaning of the term “accessibility attribute.”

*e) Claim Construction Conclusion for
“Accessibility Attribute”*

We recognize that “[t]he very nature of words would make a clear and unambiguous claim a rare occurrence.” *Autogiro Co. of Am. v. United States*, 384 F.2d 391, 396 (Ct. Cl. 1967). The Federal Circuit, however, has provided a beacon, which we have followed, to guide us in determining the proper construction when we encounter ambiguities or differing interpretations from the parties:

Ultimately, the interpretation to be given a term can only be determined and confirmed with a full understanding of what the inventors actually invented and intended to envelop with the claim. The construction that stays true to the claim language and most naturally aligns with the patent’s description of the invention will be, in the end, the correct construction.

Renishaw PLC v. Marposs Societa’ per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (citations omitted).

Based on the evidence and the analysis above, we determine that that the term “accessibility attribute” means “an attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted.” This is the construction that stays true to the claim language and most naturally aligns with the patent’s description of the invention.

*3. Biometric Signal
Characterised by Number and Duration*

All of the challenged claims include a clause that requires receiving, being configured to receive, or being capable of receiving “a series of entries of the biometric signal,” where the series is “characterised” or determined by

“at least one of the number of said entries and a duration of each said entry.”
See, Ex. 1001, 16:13–18 (for independent claim 1). We refer to these clauses collectively as the “number and duration” clauses.

These number and duration clauses all go to the embodiment of the invention that allows the administrator to require a biometric input signal that comprises “either or both (a) the number of finger presses and (b) the relative duration of the finger presses.” Ex. 1001, 10:60–63 This is the “dit, dit, dit, dah” form of biometric signal discussed in the Specification (*id.* at 11:1–7) and discussed above in this Decision. The capability for an administrator to use this disclosed embodiment exists in the claimed system and method whether the administrator chooses to use it or not.

As stated in the Specification, the administrator may use a single thumb press on a sensor for the required biometric signal. Ex. 1001, 5:60–63 (“for example, if the biometric sensor 121 in the code entry module 103 is a fingerprint sensor, then the request 102 typically takes the form of a thumb press on a sensor panel”). Alternatively, the administrator “can provide control information to the code entry module by providing *a succession of finger presses to the biometric sensor 121.*” *Id.* at 10:56–58. Thus, as disclosed in the ’705 patent, whether using a single thumb press or a succession of finger presses of variable number and duration, the input vehicle is the same – biometric sensor 121.

Patent Owner asserts that Petitioner, and the Board in its Decision to Institute this proceeding, improperly “blur the lines” between “‘knowledge-based’ security features (those based on knowledge, such as a passcode or particular pattern, and not on any attribute of the user), and a biometric signal based on the unlearnable attribute of the user.” PO Resp. 9. We

disagree. Patent Owner fails to properly understand Petitioner's, and our, analysis of the number and duration clauses.

Patent Owner asserts:

Crucially, the antecedent for this series is 'a series of entries of the biometric signal,' *i.e.*, the entries and corresponding series are 'of the biometric signal,' and the 'number of said entries and a duration of each said entry' refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information.

Id. at 9. As explained above, in our Decision to Institute, and in this Decision, we construe the number and duration clauses to require a number and duration of biometric signals because the input for these biometric signals is a biometric sensor, as disclosed in the Specification. A fingerprint sensor's ability to recognize a fingerprint is not turned off when a succession of finger presses is applied to the fingerprint sensor. Thus, contrary to Patent Owner's argument (*see* PO Resp. 10), our construction of the number and duration clauses is not based on a "knowledge-based security feature."

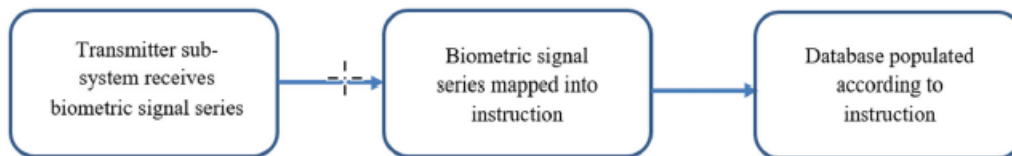
In summary, our construction of the number and duration clauses is that the number and/or duration of entries is based on entries of a biometric signal, such as a finger press on a fingerprint sensor. Based on the claim language and the Specification (*see* Ex. 1001, 10:61–63 ("the control information is encoded by *either or both* (a) the number of finger presses and (b) the relative duration of the finger presses")) (emphasis added)), this is the construction that stays true to the claim language and most naturally aligns with the patent's description of the invention.

4. *Populate the Database*

Patent Owner asserts that if and when the number and duration clause (citing clause 1(d)(1) in Petitioner's Claim Listing Appendix (Pet. 64)) is

used by an administrator to establish an authorized user, that information is “mapped into an instruction and the resulting instruction is used to populate the database of biometric signatures.” PO Resp. 11 (citing representative clauses 1(d)(2) and 1(d)(3) from Petitioner’s Claim Listing Appendix). Patent Owner also acknowledges that “the ‘populate’ limitation in claim 1 is part of that enrolling feature.” PO Resp. 11. We understand that reference to the “enrolling” feature is a reference to the administrator establishing a database of authorized users (“biometric signatures”) that will be used to match against a received biometric signal to provide access to the controlled item dependent upon the success or otherwise of the matching operation. *See, e.g.* claim 12.

Patent Owner asserts that “[t]o satisfy the requirements for antecedent claiming, ‘said series’ in clause 1(d2) must refer to the ‘series of entries of the biometric signal’ in clause 1(d1).” PO Resp. 11. Patent Owner provides the following flow diagram for populating the database:



Id. at 12 (citing Ex. 2011 ¶ 82). The flow diagram provides Patent Owner’s graphic interpretation of the three steps involved in populating the database of approved users. These basic steps apply whether the biometric signal is a single finger press or a series of finger presses.

In its claim construction arguments, Patent Owner attempts to draw a sharp distinction between a process using a single finger press, and a process that uses the number and duration of finger presses, as two technologically distinct processes. Patent Owner has not, however, cited any persuasive

evidence to support this asserted distinction. In fact, the evidence is to the contrary.

As we have noted throughout this claim construction analysis, the controlling case law is consistent in stating that the Specification is the single best guide to the meaning of a disputed term, and is, thus, the primary basis for construing the claims. *E.g.*, *Grace Instrument*, 57 F.4th at 1008. In the '705 patent, the Specification also is consistent in stating that the using a number and duration of finger presses as a biometric input signal, and using a single finger press, are done exactly the same way – both use the same biometric fingerprint sensor. *See, e.g.*, Ex. 1001, 10:56–58 (the administrator “can provide control information to the code entry module by providing a succession of finger presses *to the biometric sensor 121*”) (emphasis added).

The Specification also is consistent in stating that the system administrator establishes a database of authorized users, or authorized biometric signatures, by using appropriate software to create, or populate, the database. *See, e.g., id.* at 14:27–37.²¹ There is no persuasive evidence to which we have been directed that the biometric fingerprint sensor ceases to

²¹ The cited text from the Specification states:

FIG. 10 is a schematic block diagram of the system in FIG. 2. The disclosed secure access methods are preferably practiced using a computer system arrangement 100', such as that shown in FIG. 10 wherein the processes of FIGS. 3–4, and 6–9 may be implemented as software, such as application program modules executing within the computer system 100'. In particular, the method steps for providing secure access are effected by instructions in the software that are carried out under direction of the respective processor modules 107 and 109 in the transmitter and receiver sub-systems 116 and 117.

function as a biometric fingerprint sensor when the administrator establishes a database using the number and duration of finger presses. Patent Owner's argument is actually to the contrary in that Patent Owner asserts that the number and duration of finger presses is a biometric signal. PO Resp. 9 (“[T]he entries and corresponding series are ‘of the biometric signal,’ and the ‘number of said entries and a duration of each said entry’ refers to the entries of the biometric signal, and not an entry of some other information, such as knowledge-based information.”). This means the number and duration of entries must include a biometric component.

If the number and duration of presses did not include a biometric component, it would be simply a “knowledge-based” security measure, based on a pattern rather than based on a unique physical attribute of the user. Patent Owner asserts that such a pattern can be learned, and thus is inconsistent with the ’705 patent’s claims and disclosure. PO Resp. 7–11. Whether the software used by the administrator to populate the database of approved users relies on this biometric component is not disclosed in the ’705 Specification.

We now turn to the merits of Petitioner’s asserted Grounds of unpatentability.

D. Ground 1
Claims 1, 4, 6, 10–12, 14–17
Based on Mathiassen, McKeeth, and Anderson

Petitioner contends that claims 1, 4, 6, 10–12, and 14–17 would have been obvious over the combination of Mathiassen, McKeeth, and Anderson. Pet. 9–54.

1. Mathiassen (Ex. 1004)

We make the following finding of facts concerning Mathiassen.

Rather than using passwords or “tokens,” such as an entry card, Mathiassen discloses a portable fob-type fingerprint sensor to access secured items, such as vehicles, computers, safes, medicine cabinets, and weapons cabinets. Ex. 1004 ¶¶ 1–4, 16–18, 109–113.

Figure 8 from Mathiassen is reproduced below.

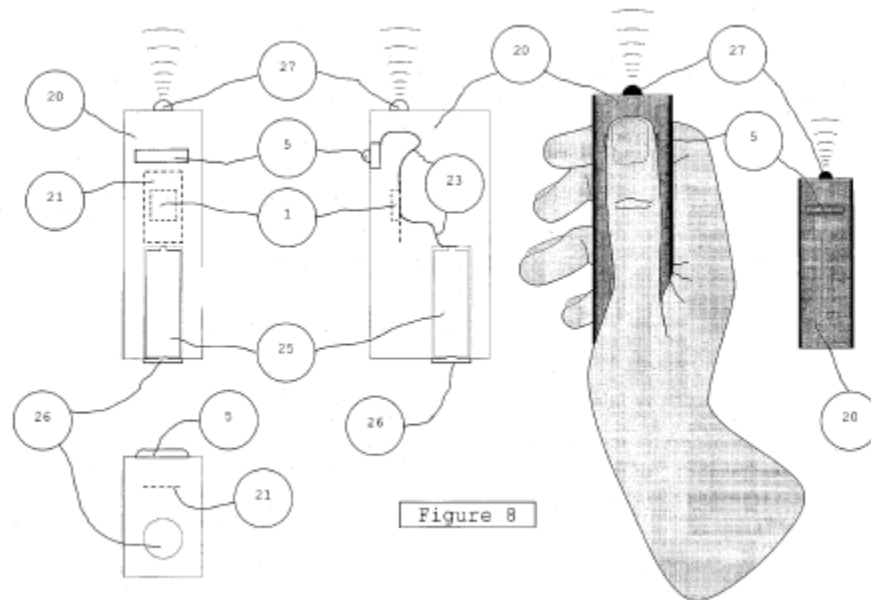


Figure 8 is a schematic illustration of a “user input device” providing access to a vehicle door. As shown in Figure 8, portable device 20 contains fingerprint sensor 5 coupled to a miniature printed circuit board 21 on which is mounted integrated circuit (“IC”) 1. Ex. 1004 ¶ 147. Thus, remote control 20 becomes a biometric sensor. *Id.* ¶ 5. Remote biometric control 20 includes battery 25 as a power supply. *Id.* ¶ 147. Battery 25 is connected to printed circuit board (“PCB”) 21 by wires. *Id.*

Remote biometric control 20 also is equipped with wireless 2-way transceiver 27. All the active components are connected to integrated circuit 1 by cables 23 through printed circuit board 21. *Id.*

Ignition control device 15 (*see* Fig. 6) is mounted inside the car on gear stick 71 or on steering wheel 72. *Id.* ¶ 148. Remote control 20 and embedded ignition control 15 are both connected to a central computer (not shown) in the car. *Id.* ¶ 149. Remote control 20 is connected to the central computer by 2-way wireless transceiver 27, while ignition control 15 is hard-wired to the central computer. *Id.*

2. *McKeeth (Ex. 1005)*

We make the following finding of facts concerning McKeeth.

McKeeth discloses a method and system for authenticating a user to access a computer system. Ex. 1005, Abstr.

McKeeth summarizes the problems with current systems for accessing computers, such as using a private identification code or password (Ex. 1005, 1:14–30),²² or a machine readable card (*id.* at 1:31–36).

McKeeth also notes that “some computer makers considered using the user’s fingerprint to authenticate and grant access to the computer system.”

Id. at 1:36–38. McKeeth recognized, however, that even using fingerprints was not without problems because “a sophisticated computer hacker may be able to copy the user’s fingerprint and provide a simulated signal to the computer system to obtain access.” *Id.* at 1:51–54.

The method and system disclosed in McKeeth provide for one or more of various types of user inputs to be used, alone or in combination, for authentication. These various inputs can be a password, a unique series of clicks of a mouse, a unique geometric pattern created by the user (*see* Figs. 3A–3D (illustrating a simple triangle, rectangle, line, or circle drawn by the

²² Citations are to column:line of McKeeth.

user), an audio sensor (for voice recognition), or an optical scanner for fingerprint, retina scans, or other biometric inputs. Ex. 1005, 2:2:53–3:12.

Figure 1 from McKeeth is reproduced below.

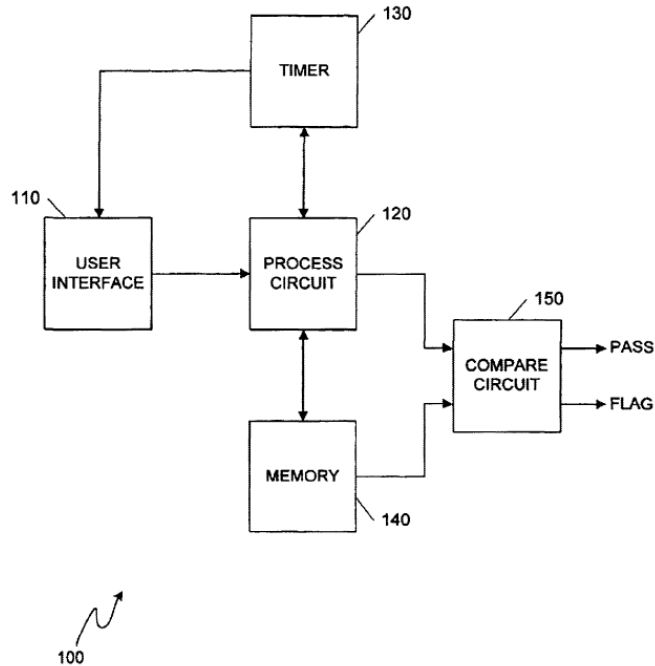


Figure 1 from McKeeth is a block diagram showing one version of a the method and system for authenticating the identity of a user disclosed in McKeeth. Ex. 1005, 2:36–37. As shown in Figure 1, computer system 100 includes user interface 110 that is operationally connected to process circuit 120. *Id.* at 2:55–57. User interface 110 may be any input device that is used to enter or communicate information to computer system 100, such as a keyboard, mouse, trackball, pointer, touch-screen, remote terminal, audio sensor, optical scanner, telephone, or any similar user interface. *Id.* at 2:57–61.

Process circuit 120 is configured to receive input signals from user interface 110. The process circuit is operationally connected with timer 130 that measures time duration between the various input signals. Ex. 1005,

3:36–38. If, for example, the user performs a fingerprint scan and/or pattern within the designated time, process circuit 120 communicates the input signals to compare circuit 150 for authentication. *Id.* at 3:52–55. Compare circuit 150 is operationally coupled to memory 140, which stores a list of legitimate user identifications (ID’s) with respective passwords, fingerprint, pattern, or any other type of security information for recognition by the computer system. *Id.* at 3:55–60. If there is a match between the user inputs, within the designated time, and stored security information, the compare circuit 150 issues a “pass” signal to computer system 100. *Id.* at 65–67.

3. *Anderson Ex. (1006)*

We make the following finding of facts concerning Anderson.

Anderson also discloses a system and method for authenticating an authorized user to access a secured device. Anderson’s disclosed system inputs an access code “via temporal variations in the amount of pressure applied to a touch interface.” Ex. 1006, Abstr.

Anderson’s method of inputting an access code uses digitizer pad 120 as a touch interface, which may include an optical scanner or thermal sensor for collecting an image of the user’s fingerprint. Ex. 1006, 5:43–44, 7:4–7. The user enters the access code as a series of pressure pulses having varying durations. *Id.* at 6:45–47. This fingerprint access code is then compared with a stored code template to determine whether they match. If they do, access is permitted. *Id.* at 6:48–54.

Anderson discloses a system where the touch interface may sense only “temporal applications of pressure,” relying on *timing* of the pressure applications for entry of the access code. Ex. 1006, 7:28–30; Fig. 4A. Alternately, as shown in FIG. 4B, the touch interface may sense both

temporal applications of pressure and variations in pressure magnitude or intensity. *Id.* at 7:34–37. Thus, the access code would be entered as a series of alternating short and long pressure applications that vary both in duration and magnitude. *Id.* at 7:37–39.

Annotated Figure 4A from Anderson is reproduced below.

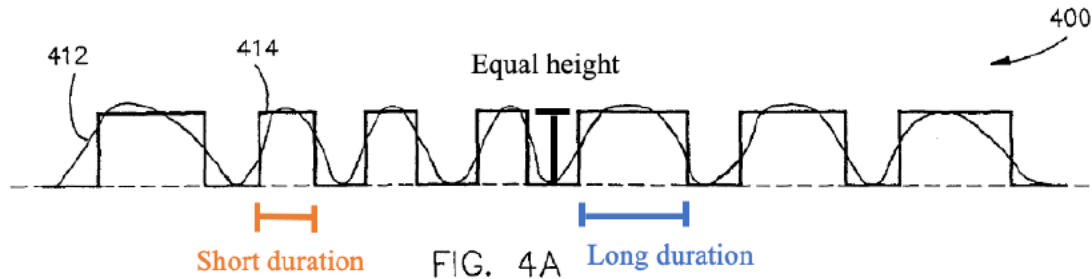


Figure 4A from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 100. As explained by Dr. Sears, in Figure 4A, “the height of each bar the same because the magnitude or intensity of the finger pressure press is not detected. However, at least some of the presses have a different duration than other presses, as represented by the width of each bar.” *Id.*

Annotated Figure 4B from Anderson is reproduced below.

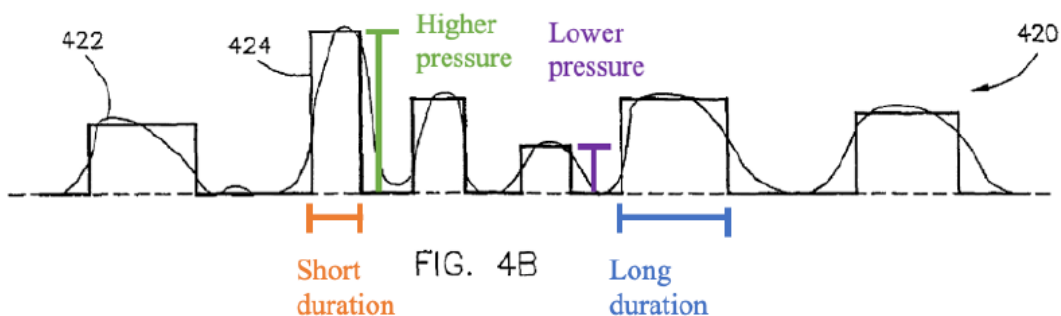


Figure 4B from Anderson is a diagram illustrating entry of an access code via temporal pressure variation. Ex. 1006, 2:65–67. The annotations are provided by Dr. Sears in his declaration testimony. Ex. 1003 ¶ 101. As

explained by Dr. Sears, Figure 4B “illustrates variations in both the amount of pressure applied using the height of each bar and the duration of the applied pressure using the width of each bar.” *Id.*

We begin our claim analysis with claim 1.

4. *Analysis of Independent Claim 1*

Petitioner provides a clause-by-clause analysis of independent claim 1, identifying where in each of the cited references, Mathiassen, McKeeth, or Anderson, the claimed element is disclosed, and why it would have been obvious to a person of ordinary skill to combine the various disclosed elements with a reasonable expectation of success. *See* Pet. 9–42.

Throughout its analysis, Petitioner cites the Declaration testimony (Ex. 1003) of Dr. Sears for evidentiary support.²³ In general, Petitioner explains the proposed combination of references as:

First, Mathiassen’s biometric security system is modified to output a duress and/or alert condition, per McKeeth, responsive to a user’s biometric signature. Mathiassen already contemplates outputting various commands based on different user-inputted biometric signals, indicating a duress and/or alert condition based on a particular inputted biometric requires only simple programming. Second, Mathiassen is modified to recognize a touch duration, per Anderson, of the fingerprint representation on the fingerprint sensor.

Reply 1.

For ease of reference and consistency, we will refer to Petitioner’s Claim Listing Appendix convention (Pet. 64–69), as did Patent Owner (*see, e.g.*, PO Resp. 11 referring to “transmitter subsystem (representative

²³ Petitioner cites this testimony as “Dec.” Pet. 3, fn 1. We will cite it, as we do all other evidence, by reference to its Exhibit number, which is Exhibit 1003.

clause 1(d1)), that series is mapped into an instruction (representative clause 1(d2)), and the resulting instruction is used to populate the database of biometric signatures (representative clause 1(d)(3))”.

Patent Owner asserts that Petitioner has not met its burden to prove unpatentability because:

(1) Mathiassen, alone or in combination with other references, does not disclose the “accessibility attribute” limitation, as properly construed, and, moreover, there is no motivation to combine Mathiassen with the other references (PO Resp. 14–25);

(2) Anderson, alone or combined with Mathiassen, does not disclose the “biometric signal duration limitation,” and, also, there is no motivation to combine Anderson and Mathiassen (*id.* at 26–32);

(3) the references, alone or in combination, do not “populate” the database according to an “instruction” (*id.* at 32–35); and

(4) there were simpler solutions available to a skilled person than the Mathiassen/Anderson combination (*e.g.*, PO Resp. 3–4, 24–25, 30–31; Sur-reply 6–17).

Patent Owner states these same arguments apply to independent claims 10, 11 and 14–17, as well as the challenged dependent claims. PO Resp. 35 (asserting that these claims “contain the ‘populating,’ ‘duration,’ and ‘accessibility attribute’ limitations, and, as the prior art cited by Apple does not teach these limitations, the cited prior art does not render these [] claims obvious as a result thereof”).

Patent Owner’s defenses are based in large part on accepting Patent Owner’s asserted claim constructions, which we have *not* done.

a) Preamble

“A system for providing secure access to a controlled item”

Petitioner asserts that “[t]o the extent the preamble is limiting, Mathiassen teaches a system for providing secure access to a controlled item.” Pet. 9 (citing Mathiassen, Abstr., ¶¶ 16, 122–123, 145–147; Ex. 1003 ¶¶ 112–113).

Patent Owner does not contest specifically Petitioner’s arguments with respect to the preamble of claim 1. *See generally* PO Resp.

Based on Petitioner’s arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests the preamble of claim 1.

b) Clause 1(a)

“a memory comprising a database of biometric signatures”

Petitioner asserts that Mathiassen discloses a stored database of tables stored in memory 7, 7A. Pet. 11–13 (citing Ex. 1004, ¶¶ 50, 147, Fig. 2B; Ex. 1003 ¶¶ 119–121).

Patent Owner does not contest specifically Petitioner’s arguments with respect to the preamble of claim 1. *See generally* PO Resp.

Based on Petitioner’s arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests the claimed memory of a database of biometric signatures.

c) Clause 1(b)

“a transmitter sub-system”

Petitioner asserts Mathiassen teaches a transmitter subsystem, including transceiver 27, fingerprint sensor 5, processor 2 (of integrated circuit 1), and non-volatile memory 7, 7A, each housed in portable control 20. Pet. 13–14 (citing Ex. 1004 ¶¶ 185–188; Ex. 1003 ¶¶ 123–126).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b).

d) Clause 1(b1)

“a biometric sensor configured to receive a biometric signal”

Petitioner asserts that Mathiassen's "fingerprint sensor 5" is a "biometric sensor for receiving a biometric signal" because it detects a finger on the sensor and processes raw images of fingerprints. Pet. 14 (citing Ex. 1004 ¶ 49; Ex. 1003 ¶¶ 127–128).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b1).

e) Clause 1(b2)

“a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute”

As discussed in detail in Section II.C.2 (Claim Construction), the term "accessibility attribute" is an "attribute that establishes whether and under which conditions, if any, access to the controlled item should be granted to a user." Thus, the attribute may, or may not, impose any conditions on permitting access.

Petitioner asserts "Mathiassen's processor 2 of the IC 1 in the portable door control 20 discloses a "transmitter sub-system controller," as recited in

claim 1. Pet 15. According to Petitioner, Mathiassen’s portable control processor is configured to match the user’s biometric signal against the database of biometric signatures. Pet. 16 (citing Ex. 1003 ¶¶ 131, 133–135). If there is a match, the processor will proceed to open (or lock) the car doors. *Id.* at 17 (citing Ex. 1004, ¶¶ 180–182); Ex. 1003 ¶ 136).

Petitioner also asserts Mathiassen’s “open door” command as modified by McKeeth’s “teaching of duress and alert conditions” discloses “or renders obvious” outputting an accessibility attribute, as claimed. Pet. 17 (citing Ex. 1003 ¶¶ 137–171).

Petitioner also asserts that McKeeth discloses a system in which “access is granted where ‘there is a match between the input and security information.’” Pet. 18 (citing Ex. 1005, 3:65–67, 3:11–28). McKeeth discloses different types of input security information, including audio sensors to detect a voice recognition and an optical scanner for fingerprint and/or retina scans. Ex. 1005, 3:1–10. Any, a combination, or all of the described types of input signals may be used to authenticate a user. Ex. 1005, 3:11–12. If the input and security information do not match the stored information, the compare circuit issues a “flag signal” indicating denial of access by the user. *Id.* at 4:2–4.

Petitioner concludes that the “collective teachings” of Mathiassen and McKeeth:

teach outputting an accessibility attribute, where the accessibility attribute may be one of an access attribute (Mathiassen and granting access to a car owner/administrator), a duress attribute (McKeeth and granting limited access along with a security alert), and an alert attribute (McKeeth and denying access along with a security alert).

Pet. 21–22 (italic font for reference names deleted throughout herein). Thus, Mathiassen combined with McKeeth suggests a more comprehensive “accessibility attribute” than Mathiassen alone.

As discussed above, Petitioner’s position is that an “accessibility attribute” without any conditions satisfies the ‘under which conditions’ construction component.” Reply 4. Based on our claim construction of “accessibility attribute, we agree with Petitioner’s position.

Petitioner concludes that Mathiassen and McKeeth “each teaches **under what conditions** access is granted.” Pet. 18. “Specifically, both references teach outputting an accessibility attribute upon there being a match of a live or access biometric signal to a stored biometric signal.” *Id.* Petitioner notes that McKeeth “teaches both a duress instruction and an alert instruction when there is no match.” *Id.*

Petitioner also provides reasoning why it would have been obvious to combine Mathiassen and McKeeth with a reasonable expectation of success. Pet. 22–24. According to Petitioner, it would have been obvious to a person of ordinary skill, that is a person with a degree in computer engineering, computer science, electrical engineering, or a related field, and with one year of relevant experience, to increase user safety of Mathiassen by providing accessibility attributes indicating duress access or alert access, as proposed in McKeeth, to thereby increase user security. *Id.* (citing Ex. 1003 ¶¶ 149, 151–161).

Patent Owner asserts that Mathiassen and McKeeth disclose only a “binary” system, without specifying the conditions under which access is permitted. PO Resp. 14–17. We disagree based on our analyses above. Our construction of the “accessibility attribute” allows for conditional access, if

any conditions are imposed, or unconditional access, if no conditions are imposed. Patent Owner's arguments fail to account for this construction.

Patent Owner also argues that there is no motivation to combine Mathiassen and McKeeth because there were simpler alternative solutions available, the existence of which undermines the motivation to combine. PO Resp. 19–23; Sur-reply 4–8. This argument is inconsistent with controlling caselaw that makes clear “[i]t’s not necessary to show that a combination is the *best* option, only that it be a *suitable* option.” *Intel Corp. v. PACT XPP Schweiz AG*, 61 F.4th 1373, 1380 (Fed. Cir. 2023) (citing *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 800 (Fed. Cir. 2021) (quoting *PAR Pharm., Inc. v. TWI Pharms., Inc.*, 773 F.3d 1186, 1197–98 (Fed. Cir. 2014) (emphasis in original)); *see also Netflix, Inc. v. DivX, LLC*, No. 2022-1083, 2023 WL 2298768, at *5 (Fed. Cir. Mar. 1, 2023) (citing *In re Mouttet*, 686 F.3d 1322, 1334 (Fed. Cir. 2012) and *In re Kahn*, 441 F.3d 977, 990 (Fed. Cir. 2006)).

The motivation-to-combine analysis is a flexible one. “[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.” *KSR*, 550 U.S. at 420 (emphasis added). And “[a] person of ordinary skill is also a person of ordinary creativity, not an automaton.” *Id.* at 421. Thus, “in many cases[,] a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *Id.* at 420. The motivation-to-combine analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court [or this Board] can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *Id.* at 418.

Here, based on our claim construction and analysis of the references, we determine that Petitioner establishes the claimed “accessibility attribute.”

Based on Petitioner’s arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b2).

f) Clause 1(b3)

“a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute”

Petitioner asserts Mathiassen teaches a “transmitter,” namely transceiver 27 of portable control 20, that is “configured to emit a secure access signal conveying information dependent upon said accessibility attribute.” Pet. 24 (citing Ex. 1004 ¶¶ 147, 186; Ex. 1003 ¶¶ 172–173).

Petitioner also asserts the IC processor in Mathiassen encrypts a command, such as “open door,” with a temporary password or key. Pet. 25 (citing Ex. 1004 ¶¶ 50, 185). Transceiver 27 wirelessly transmits the encrypted command to a transceiver at the central car computer. *See* Ex. 1004 ¶¶ 186–188); Ex. 1003 ¶ 178. Petitioner concludes that “[b]ecause Mathiassen teaches the key used to encrypt the command sent from the portable control to the ignition control/car computer changes for each transaction, the encrypted command is non-repeatable and non-replayable. Therefore, Mathiassen teaches a ‘secure access signal.’” Pet. 26 (citing Ex. 1003 ¶¶ 182–183).

Patent Owner does not contest specifically Petitioner’s arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner’s arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(b3).

g) Clauses 1(c and 1(c1))

“a receiver sub-system comprising: a receiver sub-system controller configured to: receive the transmitted secure access signal”

Petitioner discusses clauses 1(c) and 1(c1) together, and we follow this format.

Petitioner asserts Mathiassen teaches a receiver sub-system comprising “the central car computer and door lock transceivers, the central car computer, and ignition control 15.” Pet. 28 (citing Ex. 1004 ¶¶ 186–188). As asserted by Petitioner, the central car computer includes a transceiver receiving the secure access signal (the “open door” command) from the portable control. *Id.* As Petitioner states correctly “the door locks include a transceiver receiving the relayed and authenticated open door command.” Pet. 28. (citing Ex. 1003 ¶¶ 187–189; Ex. 1004 ¶¶ 149, 167, 186–187). According to Petitioner, a “transceiver” is well understood to include a receiver. *Id.* (citing Ex. 1003 ¶ 190). Petitioner concludes that Mathiassen discloses a receiver sub-system, as claimed. *Id.* (citing Ex. 1003 ¶ 191).

Petitioner also asserts that Mathiassen discloses a receiver sub-system, including the transceivers, the central car computer, and ignition control. Pet. 28–30. According to Petitioner, “a POSITA would have understood a processor performing the claimed function of receiving the signal and providing conditional access,” which is “at least equivalent to the claimed “controller.” *Id.* at 28 (citing Ex. 1003 ¶¶ 192–197).

Patent Owner does not contest specifically Petitioner’s arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(c) and 1(c1).

h) Clause 1(c2)

“a receiver sub-system control . . . configured to: provide conditional access to the controlled item dependent upon said information”

Petitioner's proposed construction in this proceeding for the phrase “conditional access” is “access based on accessibility attributes.” Pet. 6, 30; *see also* Ex. 1074, 3 (the Joint Claim Construction Statement in the related parallel litigation). We have defined the term “accessibility attribute” above and discussed its application in previous clauses. We need not repeat this analysis.

Petitioner asserts Mathiassen discloses access to a closed item, such as a door, dependent upon the information in the secure access signal. Pet. 30. According to Petitioner, because Mathiassen's commands specifically instruct a function (i.e., open door locks vs. lock door locks), the command (i.e., the “secure access signal”) includes information specific to the instructed function. *Id.* (citing Ex. 1004 ¶ 167; Ex. 1003 ¶ 200).

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(c2).

i) Clause 1(d)

“wherein the transmitter sub-system controller is further configured to:”

Similar to the analysis for clause 1(b2) discussed above, Petitioner asserts that “processor 2 of IC 1 in [the] portable door control” in

Mathiassen discloses this element. Pet. 31 (citing Ex. 1004 ¶¶ 50, 147; Ex. 1003 ¶ 202).

Patent Owner does not contest specifically Petitioner’s arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner’s arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests clauses 1(d).

j) Clause 1(d1)

“[configured to] receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;”

Petitioner acknowledges that [a]lthough Mathiassen teaches inputting a command via a series of fingerprint representations, Mathiassen does not teach determining a duration of each entry. Anderson teaches inputting an access code including fingerprint presses of varying duration.” Pet. 3.

Petitioner asserts Mathiassen discloses storing “a series of consecutive fingerprint representations generated by the fingerprint sensor signal capture and preprocessing block (5C))” that represent various “finger movements across the sensor in two dimensions.” Pet. 32 (citing Ex. 1004 ¶ 192; Ex. 1003 ¶¶ 205–210).

Petitioner relies on Anderson for the disclosure of a “series of fingerprint pressure pulses of varying duration. Pet. 33–34 (citing Ex. 1006, 6:45–48 (“For example, wherein the access code is entered by the user as a series of pressure pulses having varying durations, a predetermined tolerance may be provided for variations in the lengths of the pulses.”), 7:40–47); *see also id.* at 7:34–39 (disclosing that, “as shown in FIG. 4B, the touch interface may sense both temporal applications of pressure and variations in pressure magnitude or intensity. Thus, the access code would be entered as

a series of alternating short and long pressure applications that vary both in duration and magnitude’’)).

As we explained above in our discussion of Anderson, there can be no reasonable dispute that Anderson discloses input biometric signals that vary in number and duration.

As explained by Petitioner,

In Mathiassen, the series of directional finger movements instruct a particular command. A POSITA would have found it obvious to substitute or modify such directional finger movements with a series of presses of varying duration, as taught by Anderson, for instructing a command at portable device 20.

Pet. 36 (citations omitted).

Petitioner also provides argument and probative evidence as to why a person of ordinary skill would have combined the disclosures of the references, with a reasonable expectation that the combination would be successful. Pet. 35–36. As explained by Petitioner,

There would have been a reasonable expectation of success in modifying Mathiassen’s processor 2 in control 20, because it executes software and directs hardware for detecting and categorizing directional movement and touch/no touch. Mathiassen’s processor is already operable to detect a finger press because it receives the fingerprint representations, in the form of captured raw images, from the fingerprint sensor. *Id.* The modification therefore only requires simple programming techniques (e.g., modification of the disclosed translation program to count the number and duration of a “touch” or “no touch”) that were within a POSITA’s expertise.

Id. at 37 (citing Ex. 1004 ¶ 192; Ex. 1003 ¶¶ 224–225).

Patent Owner asserts that the “pressure pulses” in Anderson do not generate biometric signals because they are captured “as the pressure code is entered,” and are therefore not part of the pressure code itself. *See* PO

Resp. 27. Patent Owner also explains that “combining Mathiassen’s fingerprint sensor with Anderson’s pressure code does not produce the claimed invention, as any duration would apply to a nonbiometric signal.” *Id.* at 28 (citing Ex. 2013 ¶¶ 69–71). Dr. Easttom testifies that Anderson does not capture a biometric signal. Ex. 2013 ¶¶ 69–71.

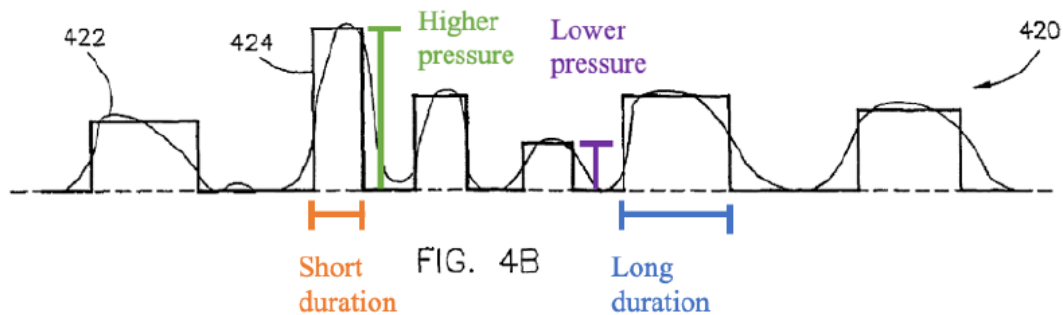
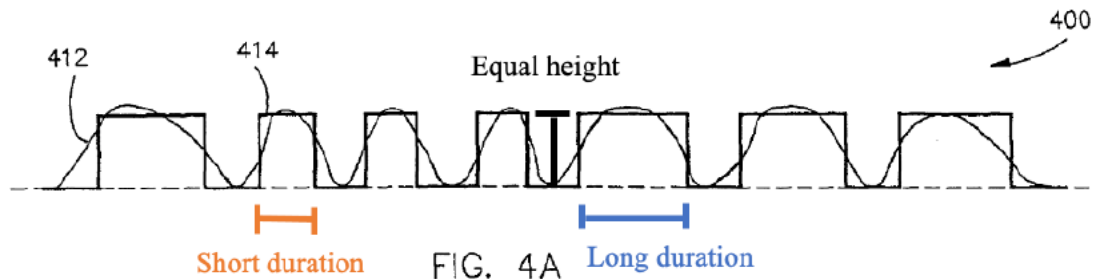
Petitioner, however, relies on Mathiassen and McKeeth for the biometric sensing, but also relies on Anderson, which suggests the benefits and options of using a number and duration of pulses as inputs. Reply 1. As explained by Petitioner,

First, Mathiassen’s biometric security system is modified to output a duress and/or alert condition, per McKeeth, responsive to a user’s biometric signature. Mathiassen already contemplates outputting various commands based on different user-inputted biometric signals, indicating a duress and/or alert condition based on a particular inputted biometric requires only simple programming. Second, Mathiassen is modified to recognize a touch duration, per Anderson, of the fingerprint representation on the fingerprint sensor.

Id.

Because Mathiassen, like the ’705 patent, uses a biometric sensor as the input device, it will detect the biometric part of the input signal, while also sensing the number and duration of inputs.

Dr. Sears’ annotated figures 4A and 4B from Anderson (*see* Ex. 1003 ¶¶ 97, 98; also discussed in Section II.D.3 of this Decision) are reproduced again below for convenient reference.



Dr. Sears testifies that Anderson’s method of inputting an access code uses digitizer pad 120 as a touch interface, which may “include an optical scanner or thermal sensor for collecting an image of the user’s fingerprint. Ex. 1003 ¶ 96 (citing Ex. 1006, 5:43–44, 7:4–7). The user then enters the access code “as a series of pressure pulses having varying durations.” *Id.* (quoting Ex. 1006, 6:45–47). This fingerprint access code is then compared with the “stored code template” in Anderson to determine a “match” to enable the desired function. *Id.* (citing Ex. 1006, 6:48–54). Dr. Sears testifies that “Anderson teaches two different access code applications: one where both the pressure of each press *and* the duration of each press is detected (Fig. 4A), and another where only the duration of each press is detected (Fig. 4B).” *Id.* (citing Ex. 1006, 7:28–39).

Dr. Sears also states, “Anderson discloses that in the second option, the ‘access code would be entered as a series of alternating pressure applications of varying duration’ where the touch interface ‘may only sense temporal applications of pressure’ and “not detect variations in pressure

magnitude or intensity.” Ex. 1003 ¶ 96 (citing Ex. 1006, 7:28–34, discussing Figure 4A in Anderson). It is Dr. Sears’ opinion that “in the first [option] the touch interface may sense both temporal applications of pressure and variations in pressure magnitude or intensity.” *Id.* (citing Ex. 1006, 7:34–37, discussing Fig. 4B in Anderson).

Patent Owner asserts that a “simpler combination” was available. PO Resp. 30; Sur-reply 4–8. According to Patent Owner, “a simpler solution would have been to add Anderson’s pushbutton to Mathiassen’s key fob.” PO Resp. 30 (citing Ex. 2013 ¶ 77). However, as explained above, “[i]t’s not necessary to show that a combination is the *best* option, only that it be a *suitable* option.” *Intel Corp.*, 61 F.4th at 1380 (citations omitted).

Based on the Petitioner’s arguments and evidence summarized above, we determine Petitioner has sufficiently shown that the cited references, as combined by Petitioner, disclose or suggest limitation 1(d1).

k) Clause 1(d2)

*“[the transmitter sub-system controller is further configured to:]
map said series [of entries of the biometric signal]
into an instruction”*

Petitioner asserts Mathiassen discloses the processor in integrated circuit 1 maps the series of biometric signal entries into an instruction by translating the series of finger movements to a command in a command table. Pet. 37–38 (citing Ex. 1004 ¶ 192). The cited disclosure in Mathiassen states:

As an additional safety feature the portable or embedded device could be equipped with means for the input of code or commands. This is achieved by defining a fingerprint storage segment in non-volatile memory (7, 7A or 7E) where the device may store a series of consecutive fingerprint representations generated by the fingerprint sensor signal capturing and pre-processing block (5C). *Movement analyzing means, in the form*

of a hardware or a software movement analyzing program module analyzes the obtained series of fingerprint representations to obtain a measure of the omni-directional finger movements across the sensor in two dimensions. Translation means in the form of a hardware or a software translation program module analyzes and categorizes the omni-directional finger movements across the fingerprint sensor according to predefined sets of finger movement sequences including directional and touch/no-touch finger movement sequences. A command table is used to translate the categorized finger movements into control signals whereby the translating means generates control signal for controlling the device, e.g. the stand-alone appliance, in response to the finger movements on the sensor.

Ex. 1004 ¶ 192 (emphases added). There can be no reasonable dispute that Mathiassen discloses a computer implemented software translation program for converting finger movements into control signals.

l) Clause 1(d3)

*[the transmitter sub-system controller is further configured to:]
populate the data base according to the instruction*

Petitioner asserts the cited references “teache[] or render[] obvious a system enrolling or populating a database of new users.” Pet. 38–42 (citing Ex. 1004 ¶¶ 71, 131, 162–167, 192; Ex. 1003 ¶¶ 231, 236–238, 241–245). Petitioner explains the mapping of the previous clause, and the “populating” of this clause as follows:

Mathiassen teaches mapping “said series” into an instruction by translating the series of movements obtained from the series of fingerprint representations into a command using the command table. (Paper 1, 37-38; Ex. 1003, ¶¶ 226-230). Mathiassen also teaches enrolling new users by generating master minutiae tables and storing the tables in memory 7,7A. (Paper 1, 38; Ex. 1003, ¶¶ 231, 233-238). Mathiassen-Anderson renders obvious populating the database according to the instruction mapped from the “said series,” as a POSITA would have found it obvious to include an enrollment command in the command table.

(Ex. 1004, [0192]; Ex. 1003, ¶¶ 233-246, pinpoint at ¶ 241). Thus, the administrator’s input series of finger movements is mapped into an instruction, i.e., an instruction to enroll a user. (Ex. 1001, 10:56–11:3 (describing an administrator’s finger press series mapping to a control signal to “[e]nroll an ordinary user”). The database is then populated “according to the instruction,” as claimed, by storing the new user’s master minutiae tables in memory. (Paper 1, 38-42; Ex. 1003, ¶¶ 231-245, pinpoint at ¶¶ 233-237).

Reply 23. Petitioner provides the following table which “summarizes how the prior art teaches Claims 1(d1)–1(d3)” (*id.*):

1(d1)-1(d3)	Petition’s Mapping
Receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry	<i>Mathiassen’s</i> processor receives information indicating a series of consecutive fingerprint representations i.e., a series of touches in a touch/no-touch sequence characterized according to the number of touches and duration of each touch (per <i>Anderson</i>).
Map said series into an instruction	<i>Mathiassen</i> translates the series of touches into a command using <i>Mathiassen’s</i> command table.
Populate the data base according to the instruction	<i>Mathiassen+Anderson</i> renders obvious generating and storing master minutiae tables for a newly enrolled user according to the instruction to enroll commanded by the series of fingerprint representations in touch/no-touch sequence of particular durations.

Id. at 24.

Patent Owner argues that “Mathiassen has no teaching that either the ‘predefined sets of finger movement sequences’ or the ‘command table’ constitute a series of received biometric signal entries that are mapped into an instruction used to populate the database as part of the enrollment process.” PO Resp. 33.

It is clear that Mathiassen's fingerprint sensor receives this series of entries of the biometric signal, similar to the '705 patent's code entry module 103 containing a biometric sensor 121 that receives a user's fingerprint. Ex. 1004 ¶ 192. Mathiassen's processor then translates the series of fingerprints received by its biometric sensor into a command, such as "open door" command, for authenticating the user to access the car doors. *Id.*

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that the prior art discloses or suggests limitation 1(d3).

m) Clause 1(e)
*"wherein the controlled item is one of: a locking mechanism
of a physical access structure or an electronic lock
on an electronic computing device"*

Petitioner asserts "Mathiassen teaches the controlled item is a 'locking mechanism of a physical access structure' (i.e., the car door locks of the central locking system)." Pet. 42 (citing Ex. 1004 ¶ 187; Ex. 1003 ¶ 247 (testifying that Mathiassen discloses a controlled item that is a locking mechanism of a physical access structure, *i.e.* a car door). We also note that Mathiassen clearly discloses use of its disclosed computer-based locking and access system on a "laptop computer," "hotel safe," "medicine cabinet," and as a "door control" in "automotive applications." Ex. 1004 ¶¶ 41–44, 109–113.

Patent Owner does not contest specifically Petitioner's arguments with respect to this limitation of claim 1. *See generally* PO Resp.

Based on Petitioner's arguments and evidence as summarized above, we determine Petitioner has sufficiently shown that Mathiassen discloses or suggests limitation 1(e).

After having analyzed the entirety of the trial record and assigning appropriate weight to the cited supporting evidence, we determine Petitioner has shown by a preponderance of the evidence that, at the time of the filing of the '705 patent, one of ordinary skill would have been motivated to combine the teachings of Mathiassen, McKeeth, and Anderson in the manner recited in claim 1.

5. *Analysis of Claims 4, 6, 10–12, and 14–17*

Petitioner also provides an element-by-element analysis of where each element in the challenged claims 4, 6, 10–12, and 14–17 is disclosed in, or would have been obvious in view of, the cited references. Pet. 42–54. For clauses in claims 4, 6, 10–12, and 14–17 that are similar to those in claim 1, Petitioner refers to its arguments for claim 1, or other claims. *See, e.g.*, Pet. 49–50 (referring to its analysis for claim 14). Petitioner also provides a reason why it would have been obvious to modify and combine the references with a reasonable expectation of success, as proposed by Petitioner. *Id.* Petitioner also relies throughout the analysis of these claims on the testimony of Dr. Sears (Ex. 1003, 1090) for evidentiary support.

Patent Owner concedes that patentability of claims 4, 6, 10–12, and 14–17 stands or falls with patentability of independent claim 1. PO Resp. 35. Thus, applying the same analysis and evidence as discussed above in the context of claim 1, we determine that Petitioner has established by a preponderance of the evidence that dependent claims 4, 6, 10–12, and 14–17 of the '705 patent would have been obvious, and thus are not patentable.

III. CONCLUSION²⁴

Petitioner has established by a preponderance of the evidence that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, that Petitioner has shown by a preponderance of the evidence that claims 1, 4, 6, 10–12, and 14–17 are unpatentable.

V. SUMMARY TABLE

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claim(s) Shown Unpatentable	Claim(s) Not shown Unpatentable
1, 4, 6, 10–12, 14–17	103	Mathiassen, McKeeth, Anderson	1, 4, 6, 10–12, 14–17	
Overall Outcome			1, 4, 6, 10–12, 14–17	

²⁴ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2022-00602
Patent 9,665,705 B2

For PETITIONER:

Jennifer C. Bailey
Adam P. Seitz
ERISE IP, P.A.
jennifer.bailey@eriseip.com
adam.seitz@eriseip.com

For PATENT OWNER:

Darlene Ghavimi-Alagha
Brian Bozzo
K&L GATES LLP
darlene.ghavimi@klgates.com
brian.bozzo@klgates.com