IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PROXENSE, LLC, Plaintiff, v. APPLE INC., Defendant.	CIVIL ACTION NO. 6:24-cv-00143-ADA **JURY TRIAL REQUESTED**

PLAINTIFF PROXENSE, LLC'S RESPONSIVE CLAIM CONSTRUCTION BRIEF

Exhibit 1033
Microsoft v. Proxense
IPR2024-00407

TABLE OF CONTENTS

I. INTRODUCTION 1
II. THE CLAIMED INVENTION 2
III. LEVEL OF ORDINARY SKILL IN THE ART 3
IV. CONSTRUCTION OF DISPUTED TERMS 3
A. "Tamper Proof Format" (730 Patent claims 1 and 8; 954 Patent claim 1) 3
B. "Access Message" (730 Patent claims 1 and 8; 954 Patent claim 1) 8
C. "A verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes an the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices" (730 patent claim 8) 13
V. CONCLUSION 17

TABLE OF AUTHORITIES

Page(s)

Cases

Alloc, Inc. v. Int'l Trade Comm'n,
342 F.3d 1361 (Fed. Cir. 2003) 3

Apple Inc. v. Motorola, Inc.,
757 F. 3d 1286 (Fed. Cir. 2014) 15, 17

Athletic Alts., Inc. v. Prince Mfg.,
73 F.3d 1573 (Fed. Cir. 1996) 13

Cordis Corp. v. Bos. Sci. Corp.,
561 F.3d 1319 (Fed. Cir. 2009) 12

Dyfan, LLC v. Target Corp.,
28 F. 4th 1360 (Fed. Cir. 2022) 14

Exxon Chem. Pats., Inc. v. Lubrizol Corp.,
64 F.3d 1553 (Fed. Cir. 1995) 10

Finisar Corp. v. DirecTV Grp., Inc.,
523 F.3d 1323 (Fed. Cir. 2008) 2

Helmsderfer v. Bobrick Washroom Equip., Inc.,
527 F.3d 1379 (Fed. Cir. 2008) 4

Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.,
381 F.3d 1111 (Fed. Cir. 2004) 12

Markman v. Westview Instruments, Inc.,
517 U.S. 370, 116 S. Ct. 1384, 134 L. Ed. 2d 577 (1996) 1

Merck & Co., Inc. v. Teva Pharms. USA, Inc.,
395 F.3d 1364 (Fed.Cir.2005) 10

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 3, 12

Rain Computing v. Samsung Electronics America,
989 F.3d 1002 (Fed. Cir. 2021) 14

Williamson v. Citrix, LLC,
792 F.3d 1339 (Fed. Cir. 2015) 14

Statutes

35 U.S.C. § 112 ..... 2, 14, 17

35 U.S.C. § 112 (6) 13

I. INTRODUCTION

This case is the *fourth* time that this Court will construe claim terms for the Patents-at-Issue largely addressing the same arguments. *Proxense, LLC v. Samsung Electronics Co., Ltd. et al*., 6:21-cv-00210-ADA (W.D. Tex.) ECF No. 43 (Claim Construction Order) and ECF 149 at 20-21 (Claim Construction Opinion); *Proxense, LLC v. Google LLC*, No. 6:23-cv-00320 (W.D. Tex.) ECF No. 59 (Claim Construction Order); and *Proxense, LLC v. Microsoft Corporation*, No. 6.23-CV-00319 (W.D. Tex.) ECF No. 66 (Claim Construction Order). The Court need not tread any new ground to reject Apple's arguments.

With respect to "tamper proof format," the Court previously considered and rejected the same arguments that Apple advances now. *See Proxense v. Samsung,* ECF No. 149 at 10-14. Even if Apple's proposed construction had not already been rejected, it excludes an embodiment from the specification, is inconsistent with the prosecution history, and conflicts with Apple's extrinsic evidence. The Court should adopt the plain and ordinary meaning of "tamper proof format."

With respect to "access message," the Court previously construed and accepted Proxense's proposed construction *three times*, in *Proxense v. Samsung, Proxense v. Google, and Proxense v. Microsoft*. Apple's arguments on "access message" confirm that Apple is not advocating for any "plain and ordinary" meaning of the term at all, but instead advocating for a position that the Court previously rejected: that the term be construed only as a message that "allows or permits access."

Apple's attempt to change prior constructions this Court previously adopted runs contrary to the doctrine of uniformity. In originally formulating the claim construction process, the Federal Circuit noted that "we see the importance of uniformity in the treatment of a given patent as an independent reason to allocate all issues of construction to the court." *Markman v. Westview Instruments, Inc*., 517 U.S. 370, 390, 116 S. Ct. 1384, 1396, 134 L. Ed. 2d 577 (1996) ("*Markman I*"); *see also Markman v. Westview Instruments, Inc.,* 517 U.S. 370, 371–73 (1996) ("*Markman*

II"). The Federal Circuit applies this principle of uniformity where, as here, there are multiple cases involving the same claim term. *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1329 (Fed. Cir. 2008). Thus, while a prior construction is not binding, it serves as persuasive authority for purposes of uniformity. The Court should adopt its prior constructions from *Proxense v. Samsung*, *Proxense v. Google,* and *Proxense v. Microsoft*.

And with respect to "verification unit," Apple asserts that the term invokes 35 U.S.C. § 112, ¶ 6, even though the claim recites sufficient structure by fully reciting the algorithm disclosed in the specification. The Court should hold the claim definite and adopt its plain and ordinary meaning, and reject Apple's arguments that a clearly defined software algorithm is indefinite.

II. THE CLAIMED INVENTION

The inventions set forth in the Patents-in-Suit (U.S. Patent Nos. 8,352,730 (the "730 Patent") and 8,886,954 (the "954 Patent") (collectively, "Family A"))[1] allow users to carry, control, protect, and use their own biometric databases on their own devices. The patents disclose new methods and systems for safely using that biometric data to securely authenticate access to applications. Biometric authentication and use of remote (e.g., web-based) applications requires trust between the user and the service provider. Safeguarding and limiting the information that is shared with multiple service providers is a necessity. The Patents-in-Suit's inventions address these issues by providing ways to *securely* use biometric information to authenticate access to sensitive information by sending messages to and receiving messages from a third-party trusted authority. Family A is directed to inventions ensuring biometric data privacy while enabling biometric authentication.

[1] As Apple notes, Proxense also alleges that Apple infringes U.S. Patent Nos. 8,646,042 and 9,679,289; but the parties do not dispute any proposed claim constructions for these patents.

III. LEVEL OF ORDINARY SKILL IN THE ART

Proxense submits that a person of ordinary skill in the art would have a Bachelor of Science degree in Computer Science, Computer Engineering, or a related discipline, and two years of experience in designing, developing, implementing, and/or deploying systems or applications on portable computing devices, including implementing or programming of software and/or firmware for biometric authentication technology. This level of skill is approximate, and more experience would compensate for less formal education, and vice versa.

IV. CONSTRUCTION OF DISPUTED TERMS

A. "Tamper Proof Format" (730 Patent claims 1 and 8; 954 Patent claim 1)

Apple's Construction	Proxense's Construction
Plain and ordinary meaning, wherein the meaning is "a format that prevents any changes to the stored data"	**Plain and ordinary meaning**

A claim term is presumed to have its plain and ordinary meaning as understood by a person of ordinary skill in the art ("POSITA") at the time of the invention in the context of the patent. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005); *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003). Apple alleges that its construction of "tamper proof format" is the "plain and ordinary meaning" of the term. At the outset, this argument is strained because a true clarification of the plain and ordinary meaning of "tamper proof format" would not need to include extreme limiters like "any changes" in the construction. Indeed, there would be no need to construe the term at all. Instead, Apple's opening brief makes clear that it is trying to construe "tamper proof format" to be much narrower than what it would ordinarily mean. Moreover, Apple's proposed construction is inconsistent with the full context of the claims and prosecution history.

Its proposal also excludes a preferred embodiment and conflicts with Apple's own extrinsic evidence. The Court should reject Apple's attempt to create an end-around the Court's prior construction of a nearly identical term.

The full claim term, in context, reads: "persistently storing biometric data of the user . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." The claim language notes storage on a medium that is persistent ("persistently storing . . . .") in a tamper proof format. Tamper proofing has the additional attribute of not being able to be subsequently altered once in memory—the limitation stating that the storage be in a "tamper proof format . . . that is unable to be subsequently altered." There is no need to construe the term, per Apple's proposal, such that the larger claim term would read as follows: "persistently storing biometric data of the user . . . **in a format that prevents any changes to the stored data written to a storage element on the integrated device that is unable to be subsequently altered**." Apple asserts the claims demonstrate that a "tamper proof format … prevents any changes to the stored data" and also prevents "creation of new data." Dkt. 46, Op. Br. at 4,5. But the claims do not recite either limitation and Apple cites no instances where any such language can be found. When read in full, Apple's proposed construction complicates the easy-to-understand nature of the claim limitation.

Apple attempts to defend this construction by mischaracterizing the specification and prosecution history to exclude embodiments. As the Federal Circuit instructs: "our court has cautioned against interpreting a claim term in a way that excludes disclosed embodiments, when that term has multiple ordinary meanings consistent with the intrinsic record." *Helmsderfer v. Bobrick Washroom Equip., Inc.,* 527 F.3d 1379, 1383 (Fed. Cir. 2008). The Court should reject Apple's arguments.

First, Apple attempts to read portions of the specification out of context to impermissibly exclude an embodiment. One embodiment is discussed in the specification as follows:

> **In one embodiment**, at least some of persistent storage 226 is a memory element that can be written to once but cannot subsequently be altered. . . . Persistent storage 226 is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. Tamper-proofing increases reliability of authentication because it does not allow any changes to biometric data (i.e., allows reads of stored data, but not writes to store new data or modify existing data). **Furthermore, data can be stored in an encrypted form**.

730 Patent, 4:29-43; 954 Patent, 5:22-35 (emphasis added).

Apple points to a single example of extrinsic evidence to support its strained reading of the specification (the "Microsoft Word" document example). Dkt. 46, Op. Br., at 7. Apple is effectively arguing that *one* embodiment in an extrinsic system (not in the specification) must now be the *only* way the claim can be construed. Even if it was proper to construe a claim term based on such extrinsic evidence, Apple admits that its example "permit[s] the stored data to be subsequently altered (e.g. by unlocking the document, changing the data, and relocking the document)." *Id*. at 7-6. An authorized user would be allowed to unlock the tamper proof document. Thus, Apple's example only shows preventing ***unauthorized changes,*** and not any changes.

The argument is also contradicted by the clear context in which "tamper proof format" is discussed in the actual embodiment from the specification. "Tamper proof format" is clearly a *functional* description, referring to various methods of preventing modifications to the data that is persistently stored. *Id.* The tamper proof format is intended generally to prevent any modifications to the stored data, and "*in one embodiment*" can be write-once memory. Apple ignores that the passage ends with "[f]urthermore, data can be stored in an encrypted form." *Id.* A specific embodiment (write once memory) should not be read into the claim term "tamper proof format" based on this disclosure.

The prosecution history does not support Apple's proposed construction. U.S. Provisional Application No. 60/637,538 (the "538 Provisional"), which is incorporated into the 730 and 954 Patents, establishes that Apple's out-of-context citations to the prosecution history of the 730 Patent do not support its claim construction position. *See* 730 Patent, 1:7-11; and 954 Patent, 1:7-14; Ex. A, 538 Provisional. The 538 Provisional states that, "By enabling Bio Key users/owners to initialize their Keys by ***permanently storing*** a master set of their personal bio data (e.g. a set of fingerprints) and then preventing that data from ever being ***viewed or tampered with in any way***, Bio Keys allow users to ***carry, control and protect their own personal bio databases***." Ex. A, 538 Provisional, at 4 (emphasis added). The Provisional also discloses storing multiple fingerprints, which would be incompatible with a system that cannot add any new biometrics. *Id*. ("Bio Keys maintain only a tiny database of bio data (e.g. 1-10 fingerprints)"). In one embodiment, therefore, "tamper proofing" allows users to "control and protect their own personal bio databases." The user's ability to control their bio database by adding and removing multiple biometrics would be lost if the memory format entirely precluded making any changes to the stored data or storing any new data.

Apple's arguments regarding the *Hsu* reference from the prosecution history are unavailing. Apple cites the Amendment filed December 5, 2011, in which, according to Apple, "the applicant distinguished [] prior art" (Hsu) during the prosecution of the 730 Patent. Dkt. 46, Op. Br., at 5. Yet, Apple ignores the fundamental flaw that the patentee detailed in distinguishing from the asserted prior art.

> "In fact, the enrollment process of Hsu consists of ***flipping a switch*** on the device to an enrollment mode, so there is no indication that this switch cannot be flipped at any point in time allowing the enrollment of additional or other biometric information. Hsu col. 2, lines 10-14. By contrast, the biometric data stored on the

> Applicant's device is ***unable to be subsequently altered***, thereby beneficially ***increasing security and eliminating the potential for tampering***." 730 Patent, Amendment F, page 12, filed December 5, 2011.

If all that is required to enroll new data on a device is "flipping a switch" then any unauthorized user finding or ***stealing*** the integrated device could simply flip that switch, add their biometrics, and be allowed access. Allowing the addition of biometrics by unauthorized users would not allow a user to "***control and protect*** their personal bio database" nor would it allow reliable authentication. The ***thief flipping the switch*** would be able to add biometrics thereby robbing the user of "***control*** [over] their own personal bio database." Furthermore, the ***thief flipping the switch*** would be authenticated the same as the legitimate user. But as the specification explains, "tamper-proofing increases reliability of authentication."

Even Apple's extrinsic evidence supports Proxense's construction, not Apple's. Apple provides "contemporaneous dictionaries" that define tamper protection as "the aspect of physical security concerned with the protection of system resources ***from unauthorized*** modification, especially where modifying or altering a component degrades system security," and define tamper proof as "designed to prevent tampering **or provide evidence of tampering**". *See* Dkt. 46, Op. Br., at 6 (citing ECF 46-10; 46-11) (emphasis added). Nothing about these dictionary definitions indicates that the plain and ordinary meaning of "tamper proof" is a format that prevents *any* changes to the stored data or any new data. The definition itself suggests that it only precludes *unauthorized* modification and/or detects unauthorized changes, which aligns with the distinctions noted during the prosecution that more is required than merely "***flipping a switch***." Even Apple admits that its own extrinsic evidence rejects its narrow proposal.

Fourth, this Court made the following observation when considering *and rejecting* a nearly identical argument from Samsung in *Proxense v. Samsung*:

> The Court finds that the "Persistently storing . . . a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered" and "a tamper proof format written to the memory that is unable to be subsequently altered" terms should be given their plain and ordinary meaning. **Defendants' construction improperly adds "permanently storing in a form that prevents subsequent writing", which would render the term "unable to be subsequently altered" meaningless.** Critically, there is no indication that the patentee intended "persistently storing" and "tamper proof" to mean "unable to be subsequently altered", but Defendants' construction would equate those terms.

Proxense v. Samsung, ECF No. 149 a t 13. Therefore, the Court should construe "tamper proof format" consistent with its plain and ordinary meaning.

B. "Access Message" (730 Patent claims 1 and 8; 954 Patent claim 1)

Apple's Construction	Proxense's Construction
Adopt the Court's prior construction in *Proxense v. Microsoft*: **No construction necessary. Plain and ordinary meaning.**	**Adopt the Court's prior construction in *Proxense v. Samsung*, *Proxense v. Google*, and *Proxense v. Microsoft*:** **Plain and ordinary meaning, i.e., a signal or notification enabling or announcing access**

Apple's arguments regarding "access message" has two main pitfalls. First, Apple misrepresents the Court's construction of the term in *Proxense v. Microsoft*. Second, Apple is clearly pushing for a narrower construction of "access message" as a signal or notification that only *allows* or *permits* access (and not announce access) when that reading is clearly at odds with the plain meaning of the claim in context. The Court should reject these arguments again.

Apple mischaracterizes the Court's prior constructions of this term in *Proxense v. Microsoft* by forgetting that this Court construed the plain and ordinary meaning of "access message" as "a signal or notification enabling or announcing access" in **two** prior claim constructions before the *Microsoft* case. First, in *Proxense v. Samsung*, the parties proposed dueling constructions of this

same exact term, and the Court adopted Proxense's construction of "access message" as: "A signal or notification enabling or announcing access." *Proxense v. Samsung*, ECF 149 at 20-21. Then, in *Proxense v. Google*, Proxense's proposed construction of "an access message … [allowing / allows] the user [access to an application / to access an application]" was:

> "Plain and ordinary meaning. No construction necessary beyond adopting the Court's previous construction of 'access message' and 'ID code' in *Proxense v. Samsung*." *Proxense, LLC v. Google, LLC.,* No. 6:23-cv-00320 (W.D. Tex. May 2, 2023), ECF 45, at 9 (Resp. CC. Brief).

Thus, Proxense identified the "plain and ordinary meaning" of "access message" as the Court's previous construction in *Proxense v. Samsung.* Maintaining its previous construction, this Court construed the longer term as:

> "No construction necessary. Plain and ordinary meaning." *Proxense v. Google,* ECF No. 59, at 3.

It was in the context of these decisions that the Court found that "access message" would be afforded its plain and ordinary meaning in *Proxense v. Microsoft* because there is "[n]o construction necessary." 6.23-CV-00319, ECF No. 66 at 2.

Proxense is asking the Court to maintain its previous construction of "access message" as "a signal or notification enabling or announcing access" like the Court did in *Proxense v. Microsoft* **and** *Proxense v, Google.* Because Apple is openly raising this same dispute again under the false auspices of a "plain and ordinary meaning" construction, the clarification is necessary. Not only is Apple clearly rejecting this Court's prior constructions, but Apple is misrepresenting that this Court rejected its own prior construction in the *Microsoft* matter even though—when viewed in context—that construction clearly adopted the prior constructions from *Samsung* and *Google*.

Apple asserts that "an 'access message' that merely announces access would not practice any asserted claims." Dkt. 46, Op. Br., at 10. It is clear that Apple is requesting this Court eliminate "announcing access" from the plain and ordinary meaning of "access message." This request is at odds with the claim's own descriptions of what the "access message" does. As Apple's own citation to the 954 Patent makes clear, the claim term reads:

- "receiving, at an application, an **access message** from the trusted authority ***indicating*** that the trusted authority successfully authenticated the one or more codes and other data values sent to the third party and ***allowing the user access to the application***" Dkt. No. 46, Apple. Op. Br., Ex. 3 ('954 patent), claim 1.

Thus, the "access message" clearly also *indicates* that there is successful authentication; but Apple's proposed "plain and ordinary" construction would read that phrase out of the term. The construction of a claim term must consider all words and phrases that are part of the term, but Apple's construction fails to do so. *Exxon Chem. Pats., Inc. v. Lubrizol Corp*., 64 F.3d 1553, 1557 (Fed. Cir. 1995) ("We must give meaning to all the words in [the] claims."); *Merck & Co., Inc. v. Teva Pharms. USA, Inc*., 395 F.3d 1364, 1372 (Fed.Cir.2005) ("A claim construction that gives meaning to all the terms of the claim is preferred over one that does not do so.").

Contrary to Apple's assertions that "announcing access … would not practice any asserted claims", the words "allowing" and "allows" as used in this context can be understood to mean both "causes access to be permitted" and "announces that access is permitted." The latter would permit the application to move to the next step or inform (e.g., check appropriate age before granting access) a party that access was permitted (e.g., pop up a window to inform a user). As this Court already held, the access message "can have the effect of moving the user to the next step of providing information (like providing the user's age), ***which is more than just enabling access***." *Proxense v. Samsung*, ECF 149 at 21 (emphasis added) (citing 730 Patent at 7:18–21).

Moreover, Claim 12 of the 730 Patent (not asserted) also recites the steps of receiving an "access message" and allowing access "*in response to a positive* access message." Again, when read in the context of the entire patent, the "access message" does more than just permit access (as Apple suggests). Instead, these examples are most consistent with a construction that the access message can be "indicating" (*i.e.* announcing) that access is enabled, but that can *also* have enable access.

Apple falsely asserts that the specification of the patents do not support Proxense's (and this Court's) previous construction of the term. This Court already found that Apple is demonstrably wrong. *See Proxense v. Samsung*, ECF 149 at 21-22. The specification discloses several examples of "access message" as having an effect other than just permitting access. For example, an "access message" can be:

- An LED: "In one embodiment, LED 130 can **also confirm that** . . . **authentication has completed**." 730 Patent 3:33-35; 954 Patent 4:26-28. The embodiment here teaches that the access message is simply "confirm[ing]" successful authentication; not only permitting access.

- A pop-up window: "Response to successful authentication of the key, access is allowed 470 to application. In the slot machine example, a **new pop-up window can be spawned to indicate a successful age verification**." 730 Patent 6:28-31; 954 Patent 7:23-26. Again, the embodiment here teaches that the access message is "indicat[ing]" a successful verification.

- A signal or notification that leads another element of the system to enable access: "Authentication module 310 can send a message to application 330, **or otherwise allow access** to the application, responsive to a successful authentication by trusted key authority 320." 730 Patent 5:23-26; 954 Patent 6:15-17.

- A signal or notification that indicates access is successful *after* authentication is already completed: "In one embodiment, application module 330 **allows access** by a user **after receiving a message** from authentication module 310." 730 Patent 5:34-36; 954 Patent 6:29-31).

- A signal or notification that simply moves the user onto the next step of the authentication process: "**If authentication is successful**, the trusted key authority **sends an access message** to the application to allow user access **and/or provide**

> **additional information from the profile** (such as the user's age)." *E.g.,* 730 Patent 7:18-21.

The Court heard the same arguments that Apple now makes that "access message" must be limited to only "allow" access in *Proxense v. Samsung* and *Proxense v. Google* and dismissed them both times. That Apple now tries to justify its narrow construction by claiming that it is the same as the plain and ordinary meaning is just an attempt to distract away from its true request. Apple presents no compelling reason for this Court to deviate from its previous rulings.

Finally, Apple fails to properly apply the law regarding prosecution history disclaimer. The statement from the prosecution history that Apple cites: "[t]he user is allowed access responsive to receipt of an access message from the agent that authenticates the code" does ***not*** exclude "announcing access" from the claimed invention. Apple asserts that this statement excludes "announcing access" because the statement does not discuss "announcing access." Apple. Br. at 12. However, to disavow or disclaim the full scope of a claim term, the patentee's statements in the prosecution history must amount to a "clear and unmistakable" surrender. *Cordis Corp. v. Bos. Sci. Corp*., 561 F.3d 1319, 1329 (Fed. Cir. 2009). The above statement was about one embodiment of the claimed invention and neither included nor excluded other embodiments. *See e.g. Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc*., 381 F.3d 1111, 1117 (Fed. Cir. 2004). It was not intended to cover the full scope of the "access message" term – the specification provides the full scope of the term through its several embodiments; not via a single embodiment as Apple asserts. No express disavowal by Proxense ever limited the claim term to only "enabling access." The specification of the Family A patents is clear that announcing access is within the term's scope, and this statement does not limit the Family A specification. *Phillips,* 415 F. 3d at 1318 ("because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and

thus is less useful for claim construction purposes."); *see also Athletic Alts., Inc. v. Prince Mfg.*, 73 F.3d 1573, 1580 (Fed. Cir. 1996) (ambiguous prosecution history may be "unhelpful as an interpretive resource").

In short, Apple offers no new reasons for this court to deviate from its prior determinations as to the plain and ordinary meaning of "access message." Accordingly, Apple's attempts to do so should be rejected for the same reasons identical attempts were rejected in *Proxense v. Samsung, Proxense v. Google,* and *Proxense v. Microsoft*. The Court should thus adopt its prior construction of "access message" here.

C. "A verification unit, in communication with the memory, receives scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes an the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices" (730 patent claim 8)

Apple's Construction	Proxense's Construction
This is a means-plus-function term under 35 U.S.C. § 112 (6). **Function: (1) receives scan data from a biometric scan for comparison against the biometric data, and (2) if the scan data matches the biometric data, wirelessly sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices** **Structure: Indefinite.**	**No construction needed; plain and ordinary meaning beyond any terms that the Court previously construed in *Proxense v. Samsung*.**

Apple asserts that "verification unit" invokes 35 U.S.C. § 112 ¶ 6, because "unit" is a nonce word. Apple ignores that "§ 112 ¶ 6 will apply if the challenger demonstrates that ***the claim term***

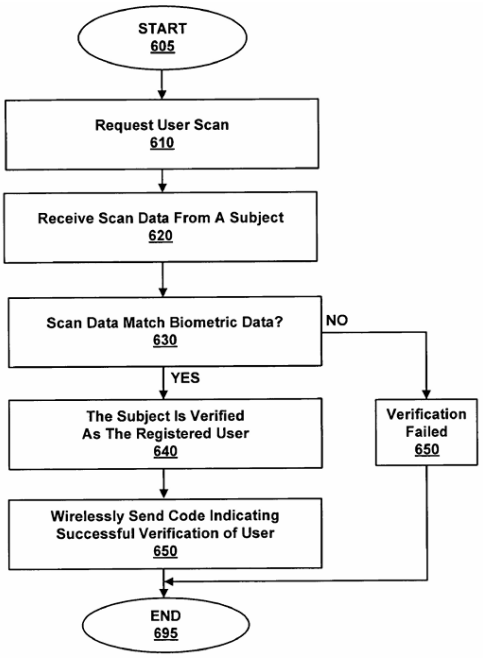
fails to recite sufficiently definite structure or else recites function ***without reciting sufficient structure for performing that function***." *Rain Computing v. Samsung Electronics America*, 989 F.3d 1002, 1005 (Fed. Cir. 2021) (citing *Williamson v. Citrix, LLC,* 792 F.3d 1339 (Fed. Cir. 2015) (cleaned up and emphasis added)). Accordingly, the relevant inquiry is whether this claim recites a sufficiently definite structure in the context of a software patent. As such, while Apple's expert Dr. Creed's testimony asserts that 'verification unit' has no well-understood meaning in the art, such testimony is insufficient to rebut the fact that the rest of the term recites sufficient structure when viewed in the context of the specification, especially where Dr. Creed states that a POSITA is an experienced engineer with years of experience. Dkt. No. 46-5 ¶ 32.

The term has structure in context. Apple asserts "verification unit" corresponds to "validation module 224." Apple. Br. at 15. The specification of the 730 Patent states that, "as will be apparent to one of ordinary skill in the relevant art, ***the modules***, features, attributes, methodologies, and other aspects of the invention can be implemented as ***software, hardware, firmware or any combination of the three***." 730 Patent, 8:58-61. Accordingly, per Apple's assertions and the 730 Patent itself, the "verification unit" is <u>code implemented as software, firmware or some other application executed by hardware</u>. "Unlike in the mechanical arts, the specific structure of ***software code and applications is partly defined by its function***." *Dyfan, LLC v. Target Corp.*, 28 F. 4th 1360, 1368 (Fed. Cir. 2022) (emphasis added). In determining whether such limitations recite sufficient structure, the Court is to look "to the functional language to see if a person of ordinary skill would have understood the claim limitation as a whole to connote sufficiently definite structure." *Id.* Furthermore, "to one of skill in the art, the '***structure' of computer software*** is understood through, for example, ***an outline of an algorithm, a flowchart, or a specific set of instructions or rules.***" *Apple Inc. v. Motorola, Inc.,* 757 F. 3d 1286**,** 1298 (Fed.

Cir. 2014) (emphasis added). "A limitation has sufficient structure when it recites a claim term with a structural definition that is either provided in the specification or generally known in the art." *Id.* at 1299.

As demonstrated below, Claim 8 itself fully recites the algorithm for verifying a subject disclosed in the 730 Patent, and thus recites a sufficiently definite structure.

The specification presents the algorithm in FIG. 6, which the 730 Patent describes as "illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention." 730 Patent, 2:51-53; *see also* 6:65-67 ("FIG. 6 is a flow chart illustrating a method 600 for verifying a subject presenting the biometric key according to one embodiment of the present invention."). "The methods of the present invention may be performed in hardware, firmware, software, or any combination thereof operating on a single computer or multiple computers of any type." 730 Patent, 7:35-38. Accordingly, FIG. 6, and the following accompanying description in the specification, is the code or application to be executed by the "verification unit".



"FIG. 6 is a flow chart illustrating a method 600 for verifying a subject presenting the biometric key according to one embodiment of the present invention. In response to an authentication request, a user scan is requested 610 (e.g., by a blinking LED). Once the subject provides a fingerprint, scan data is received 620. Scan data is compared for a match 630 to previously-stored biometric data. If there is no match, then verification fails 650.

If there is a match, the subject is verified 640 as the user. The code indicating a successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230)." 730 Patent, 6:65-7:9

Claim 8 directly incorporates the above algorithm. As shown in the below tables, both FIG. 6 and the accompanying discussion within the specification are fully recited in claim 8.

730 Patent 6:65-7:9	Claim 8
"Once the Subject provides a fingerprint, Scan data is received 620." 7:2-3	"receives scan data from a biometric scan"
"scan data is compared for a match 630 to previously-stored biometric data." 7:3-4	"for comparison against the biometric data"
"If there is a match, the subject is verified 640 as the user. The code indicating a successful verification is wirelessly sent 650 from the biometric key (e.g., by RF communication module 230)." 7:6-9	"sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority"

FIG. 6	Claim 8
"Receive Scan Data From a Subject 620"	receives scan data from a biometric scan
"Scan Data Match Biometric Data? 630" "Subject Is Verified As The Registered User 640"	for comparison against the biometric data
"Wirelessly Send Code Indicating Successful Verification of User 650"	"sends one or more codes from the plurality of codes and the other data values for authentication by an agent that is a third-party trusted authority"

Because the "verification unit" recited in claim 8 is a software limitation that fully recites the algorithm disclosed in the specification, claim 8 recites a sufficiently definite structure for the "verification unit" and does not invoke § 112, ¶ 6. Apple, however, demands more without adequate legal basis. "Requiring traditional physical structure in software limitations lacking the term means would result in all of these limitations being construed as means-plus-function limitations and subsequently being found indefinite." *Apple Inc,* at 1299. At the very least, the specification provides sufficient structure, per the above, to prevent a finding of indefiniteness.

In view of the foregoing, the Court should hold claim 8 definite and adopt the term's plain and ordinary meaning.

V. CONCLUSION

For the foregoing reasons, the Court should adopt Proxense's proposed constructions.

Dated: November 27, 2024

Respectfully submitted

By: */s/David L. Hecht*

David L. Hecht **(Co-Lead Counsel)**
dhecht@hechtpartners.com
Hecht Partners LLP
125 Park Avenue, 25th Floor
New York, New York 10017
Telephone: (212) 851-6821

Brian D. Melton (**Co-Lead Counsel**)
bmelton@susmangodfrey.com
Geoffrey L. Harrison
gharrison@susmangodfrey.com
Meng Xi
mxi@susmangodfrey.com
Susman Godfrey L.L.P.
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 653-7807
Facsimile: (713) 654-6666

Lear Jiang
ljiang@susmangodfrey.com
Susman Godfrey L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067-6029
Telephone: (310) 789-3100
Facsimile: (310) 789-3150

Counsel for Plaintiff Proxense, LLC

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on November 27, 2024, all counsel of record who have appeared in this case are being served with a copy of the foregoing and all ancillary documents filed concurrently herewith and referenced herein via CM/ECF.

/s/ David L. Hecht
David L. Hecht

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

PROXENSE, LLC, Plaintiff, v. APPLE INC., Defendant.	Civil Action No. 6:24-cv-00143-ADA **JURY TRIAL DEMANDED**

DECLARATION OF DAVID L HECHT IN SUPPORT OF PLAINTIFF'S RESPONSIVE CLAIM CONSTRUCTION BRIEF

I, David L. Hecht, counsel for Plaintiff Proxense, LLC, am over 18 years of age, and make this declaration based upon personal knowledge. If called to testify as a witness, I could and would testify competently to the same. I submit this declaration in support of Plaintiff's Responsive Claim Construction Brief.

1. Attached hereto as Exhibit A is a true and correct copy of a document filed within the 538 Provisional Application.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed in Livingston, New Jersey, on November 27, 2024.

Dated: November 27, 2024

/s/ David L. Hecht

David L. Hecht
Counsel for Plaintiff Proxense, LLC.

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on November 27, 2024, all counsel of record who have appeared in this case are being served with a copy of the foregoing and all ancillary documents filed concurrently herewith and referenced herein via CM/ECF.

/s/ David L. Hecht
David L. Hecht

EXHIBIT A

Margent Development, LLC

PDK Bio Key Technology

An extension of Margent's Personal Digital Key Technology

Technology Whitepaper

Origination date:
November 25th, 2004

Confidential

The information provided in this document concerning the Personal Digital Key (PDK™) is the exclusive property of Margent Development, LLC. Recipient hereby acknowledges that such information is confidential and privileged and will not be disclosed, copied, distributed or used without the express written consent of Margent Development, LLC.

Margent Development, LLC - PDK Bio Key

Origination date: 11-25-04

Background:

The original Personal Digital Key (PDK) design and patent applications, defined a proximity-based technology enabling many unique and powerful capabilities. Providing users with the ability to wirelessly, effortlessly, and efficiently lock/unlock protected items (e.g. digital content, digital storage devices, digital transactions, digital access, etc. - see earlier patent applications for details) the technology revolutionized the securing of such items.

The original PDK (standard PDK or non-bio PDK) was intended for use in transactions requiring low-to-medium levels of security, and was primarily geared towards situations where the goal was to ensure protected items were only accessible when their associated Keys were detected. Therefore, one of the technology's fundamental premises (and "promises") was that every PDK Key was uniquely identifiable.

What standard PDK did *not* enable was an ability to guarantee that a user attempting to utilize a specific Key was actually that Key's valid owner. So, in summary, the standard PDK technology authenticates *Keys*, but not the *individuals* using them.

Biometric ID security products, such as those utilizing fingerprint or retinal scan technologies, are currently used to identify and authenticate individuals. Yet while those technologies are quite accurate and functional, they introduce a number of inconveniences and privacy-related problems.

Biometric authentication uses can generally be categorized as being in one of two environments - "closed-loop" or "open-loop". An example of a closed-loop environment is one where a specific key is associated with a specific car. Closed-loop uses tend to be relatively simple in nature to configure and use. An example of an open-loop environment is one where any individuals wishing to shop at a particular store must be able to be authenticated during check-out. Open-loop uses generally pose far more, and complex, problems/issues.

To utilize biometric technologies such as fingerprint or retinal scanners, entities must first acquire scanning equipment for each participating location. Then, to prepare individuals to utilize the technologies, they must have each "enroll" - proving their identity (by showing a driver's license, or similar) and providing a sample of their bio data for storage within the entity's bio database. Once stored, the data is accessible for future use as needed.

Typical day-to-day use of such technologies (illustrated using fingerprint scanners as the example) involves a user placing their finger on the entity's scanning equipment, having it scanned and validated (ensuring a "clean" read), waiting for the equipment to compare the read to its bio database of previously stored scans/reads looking for a match, and finally returning with a response defining the read's authenticity ... <u>and the user's</u>. These bio databases, often containing <u>vast</u> quantities of records, may be located either on-site or remotely.

This entire open-loop model is fraught with problems, the most critical of which involves the enrollment process. For <u>every</u> new entity, the enrollment process must be repeated, representing a considerable hassle to both parties. But much more importantly, it places a significant burden on entities to securely and accurately manage the process (and acquired data), and opens individuals up to ever-increasing levels of risk.

Closed-loop environments, though generally much simpler, do sometimes have problems also. A simple example might include managing weather-related wear & tear when using fingerprint scanners in outdoor environments (such as on a car for keyless entry).

Background (continued):

A summary of the problems inherent to current biometric ID technologies includes:

- Most individuals are simply not comfortable giving their bio data (fingerprints, etc.) to third parties ... especially for permanent storage. Doing so represents a major concern for many individuals as it is obvious that bio data, unlike almost any other unique personal identifier, cannot be changed if ever breached.
- For open-loop systems, individual wishing to utilize such technology must go through an "enrollment" process (where their bio data is added to an entity's bio database) for every entity with which they wish to participate. This process, which is time-consuming and usually viewed as a hassle and an annoyance, results in a serious reluctance to "sign-up", and greatly slows the acceptance of such technologies. And worse, it repeatedly reminds users of the privacy-related problems to which they may be exposing themselves. And this exposure is real and growing - as every time a user enrolls somewhere, they have released their most private "ID" to one more third-party's confidence.
- Every entity wishing to utilize such technology must acquire and maintain its own scanning equipment (a potentially expensive endeavor in high-volume locations such as grocery stores), build and maintain its own bio database, properly train personal on the enrollment process, and install critically-important safeguards on the bio data being acquired. Each of these tasks represents significant, expensive, and time-consuming commitments ... which not only have no end, but continue to expand indefinitely.
- Because these bio databases (maintained by independent entities) must contain bio data for every participating individual, they tend to be extremely large - often resulting in inefficient and slow searches.
- As individuals must *physically* interact with an entity's scanner during transactions, the process is inherently more cumbersome to implement than proximity-based technologies such as PDK's (where users need only be within a predefined range to engage). Additionally, certain individuals are reluctant to touch public surfaces (where many others have also touched) because of the potential for germ transmission (during flu season for example).

Because of the above problems - individuals' reluctance to give out bio data (and general mistrust of the overall concept) in particular - biometric technologies are being adopted slowly, and will likely *never* be accepted in many locations where their underlying value would otherwise be greatly beneficial. A technology combining PDK's inherent proximity-based advantages with true Key-based biometric authentication capabilities, would therefore represent a powerful new option for uniquely, efficiently and conveniently identifying individuals ... while fully protecting and respecting their privacy.

Margent Development, LLC - PDK Bio Key

Origination date: 11-25-04

The Invention:

The invention, the PDK Bio Key (Bio Key or Key), is an alternative to the standard (non-bio) PDK technology. Bio Keys are basically standard PDK Keys ... incorporating integrated biometric readers/scanners (e.g. fingerprint scanners). Bio Keys can function in place of standard Keys for any previously-defined PDK use, but are also able to provide biometric authentication of users when needed.

The underlying PDK Bio Key principle and technology is directly based on that of standard PDK Key and Reader/Decoder Circuits (RDCs) technology - the underlying concept of associating PDK Keys with digital content, storage devices, transactions, access, etc. ("protected items"), and utilizing RDCs to detect and validate such associations, remains. However, by adding the biometric identification capabilities, entirely new uses unfold and the technology's scope is widened. And importantly, the design changes required to implement the PDK Bio Key technology are almost completely limited to the technology's Key component.

By enabling Bio Key users/owners to initialize their Keys by permanently storing a master set of their personal bio data (e.g. a set of fingerprints) and then preventing that data from ever being viewed or tampered with in any way, Bio Keys allow users to carry, control and protect their own personal bio databases. Then, with the initialization complete, when needed for a PDK-based transaction, users can utilize the stored data to effectively authenticate themselves to their Keys.

During normal use, a Bio Key's integrated biometric scanner/reader acquires a user's bio data, compares it to the permanently/previously stored data and uses the results to either enable or inhibit the Key's ability to attempt a basic PDK authentication process with an RDC (as defined in earlier PDK patent applications). In essence, if the scanned bio data matches the data stored in the Bio Key's memory locations (internal bio database), the Key will function like any standard PDK Key (meaning the Key will communicate with an RDC, wirelessly authenticating and establishing a secure two-way link ... and allowing access to protected items). If no match is found, the Key will be inhibited from communicating with the RDC.

Important to note is that <u>no actual bio data ever leaves a Bio Key in any way, shape, or manner</u>. The <u>only</u> location the biometric data is ever stored is inside the Key itself ... and it can never be viewed or read *from* the Key (only the Key's internal circuitry can access it when needed for authentication procedures). This means Bio Key users are always in total control of their own private and critical bio data. Additionally, because Bio Keys maintain only a tiny database of bio data (e.g. 1-10 fingerprints) in their internal memory - relative to the thousands of records that might be located, for example, in a grocery store's database - when asked to perform a comparison, the process occurs extremely fast and reliably.

A separate/inherent advantage of the PDK Bio Key technology is that Bio Keys are totally useless (and therefore secure) in the event they are ever lost or stolen. Since any wrongfully-attempted bio scan (by a thief, etc.) would yield data not matching anything stored within a Key's internal database, the Key would not function ... thereby preventing access to any associated protected items.

As an enhancement, the PDK Bio Key technology also defines a secondary authentication process where Keys are "registered". Registering a Key signifies the authenticity of the Key's owner has been validated by a third party. Additionally, once registered, a Key's *status* can also be tracked. While this level of authentication is not required in many circumstances, its availability significantly enhances the technology's capabilities and breadth of use.

Margent Development, LLC - PDK Bio Key

Origination date: 11-25-04

The Invention (continued):

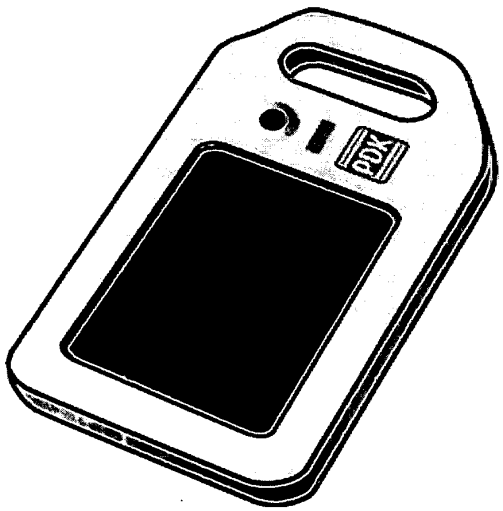
The PDK Bio Key technology's unique combination of proximity and biometric authentication capabilities enables a wide range of new/enhanced uses (in addition to any previously-defined PDK uses). Some examples include:

- Keyless entry to homes, business, automobiles (or similar).
- As an enhanced replacement for any ATM, banking, or credit-card function (or similar).
- Wherever biometric ID-based access is desirable, but impractical due to weather (or similar).
- Wherever proximity-based access is desirable, but impractical because of the level of security required.
- Wherever smart cards could be used, but are not because of their lack of biometric ID capabilities.
- Many other situations and environments where proximity and/or biometrics can enhance (or make possible) a process or experience.

In summary, the PDK Bio Key technology solves significant problems inherent to currently-available biometric technologies. It requires only a single "enrollment" process, it limits the locations at which an individual's bio data is stored to only one - the owner's personal Bio Key, and it eliminates the need to provide such data to any third-party ... ever.

PDK Bio Keys provide a powerful and elegant solution for authenticating a Key's owner, in both closed and open-loop environments, while retaining the advantages inherent in PDK's basic proximity-based design. The technology makes using biometric data for user authentication, a safe, simple and efficient process. And importantly, PDK Bio Keys enable users to maintain total control over their personal bio data.

An example PDK Bio Key
(many options exist)



Margent Development, LLC - PDK Bio Key

Origination date: 11-25-04

Design Overview:

Specifications Summary

A PDK Bio Key (Bio Key or Key) is the result of combining a standard PDK Key (as defined in previous PDK patent applications) with a biometric reader/scanner, providing a proximity-based, wireless, digital "key" able to (optionally) biometrically confirm its owner's identification. Primary specifications include:

- A PDK Bio Key is functionally identical to a standard PDK Key, but is also capable of performing a biometric authentication of its owner and using the results to effectively enable/disable itself.
- In addition to the push button typically located on a standard PDK Key, Bio Keys also include a biometric scanner/reader (Bio Reader) such as a fingerprint reader, an optional LED (while an LED is used in all included examples, other functionally-similar options could be utilized if desired), and an optional rechargeable-battery interface (because Bio Key's processing requirements and associated battery-draw is greater than that of standard PDK Keys, this option may be included on some models).
- In order to utilize a Bio Key's biometric capabilities, the intended user/owner must first perform an Owner Initialization Procedure (OIP). An OIP, which can only be run one time, consists of reading, verifying and permanently storing a number of bio scans (e.g. fingerprints) in the Key's internal bio database. While the OIP may allow for corrections (e.g. re-reads) *during* the process, once completed, any data acquired is permanently stored ... unable to ever be modified, deleted, added-to, viewed, or (externally) read. If an OIP is incorrectly completed, the Key must be discarded. These "restrictive" features are designed to prevent tampering, ID theft, forgery, etc. (see below for "restrictive" feature implementation details).
- In addition to the initialization procedure, an Owner Confirmation Procedure (OCP) is also available (for optional use). The OCP enables an individual's newly-scanned bio data to be compared to the bio data stored during the OIP, enabling third-parties to validate the authenticity of the stored data. An OCP provides the basis for the technology's optional Key Registration (KR) process.
- Internal Bio Key procedures utilize the built-in LED to guide users through procedural steps (by using specific colors, pulsing schemes, etc.). The LED also enables third-party observers to easily verify whether procedures are being correctly performed (in particular the OCP).
- For basic/ongoing use (after completion of an OIP), the LED also notifies owners whenever an RDC (with which a Key is attempting to communicate) requests a Basic Owner Authentication (BOA). Once such a request is made, the RDC simply waits until the Key has performed a valid BOA ... or times-out (or similar) because it could not. A BOA consists of acquiring newly-scanned bio data from the user and comparing it to the bio data stored within the Key's internal bio database during the OIP. Assuming a valid BOA - *meaning the Key's owner was authenticated* - the Key is allowed to respond to the RDC and complete a typical PDK Key-to-RDC authentication procedure (identical to that followed by any standard, non-bio, PDK Key). If a valid BOA was not completed, the Key is inhibited from communicating with the RDC, and therefore unable to provide access to the protected item.
- When desired, an Enhanced Owner Authentication (EOA) procedure may be performed (in addition to the BOA described above). The EOA process, performed after a successful BOA is completed, adds verification of a Key's formal registration and current status, to the authentication process.
- If desired, Bio Keys can utilize an "active time" feature, where the *time since last BOA* is transmitted as part of the basic PDK Key-to-RDC authentication process. Among other uses, this timing information allows a Key to respond to an RDC BOA request up to a set period of time *after* a BOA has been completed. An example of where this may be useful is illustrated in employing a Bio Key to unlock and/or start an automobile. Walking through a parking lot towards their car a user could complete the BOA process - preparing the Key to automatically respond to *door-open* and *engine-start* requests - before ever reaching the car.

Design Overview (continued):

- If desired, RDCs can utilize an "in-range auto validate" feature, where after completing authentication of a newly-detected Key (one that just came into range), the RDC begins a regular/periodic check for its presence. As long as the Key remains in range (is detected on each check), no further BOAs are required from the Key (the Key's other authentication features, however, remain fully functional). If, though, it is determined that the Key has moved out of range, upon its return a BOA will be required (the next time the RDC needs to communicate with the Key). An example of where this may be useful is illustrated in employing a Bio Key to control access to a PDK Hard Drive. When first coming into range of the drive, a user would be required to perform a BOA. But then, as long as the user remained in the drive's range, no additional BOAs would be required (regardless of how many other PDK-related functions the user performs).
- If desired, RDCs can utilize an "OIP required" feature, where the assignment of new Bio Keys to a device (such as a hard drive, door access mechanism, digital file, etc.) is prohibited if the Key in question has not yet been initialized (the OIP has not been completed).
- If desired, RDCs can utilize an "registration required" feature, where the assignment of new Bio Keys to a device (such as a hard drive, door access mechanism, digital file, etc.) is prohibited if the Key in question has not yet been registered (the KR process has not been completed).
- As with standard PDK Keys, to ensure total protection of the critical data routinely handled by the technology (Key identifiers, fingerprint or other bio data, etc.), PDK Bio Keys may utilize combinations of technologies such as public/private key encryption & decryption, secure hash algorithms, message authentication codes, challenge/response algorithms, etc. to establish, authenticate, and secure two-way communications between themselves and RDCs.
- As with standard PDK Keys, design mechanisms such as one that would immediately erase a Bio Key's internal memory in the event it is physically opened (as might occur if someone were attempting to tap into a Key's internal memory/circuitry) may also be utilized.

NOTES:

- *For clarity and simplicity, many biometric examples referenced in this document are illustrated using fingerprint-based technology. PDK Bio Key technology, however, is not limited to only fingerprints/fingerprint technology. Bio Keys may utilize <u>any</u> potential biometric technology and data available (e.g. retinal scan, facial recognition, etc.).*
- *While the above-referenced examples all refer to PDK's common/typical wireless implementation, as defined in earlier PDK patent applications, wired or physical-contact versions of PDK Bio Keys can also be produced if desired. These alternatives might prove appropriate, for example, in situations where large quantities of Keys could potentially be in the same general field-of-view, making it difficult or slow to establish and authenticate communications.*

Authentication-Levels Summary

PDK Bio Key technology is capable of providing multiple/various levels and types of authentication depending on whether its biometric capabilities are used, the level and type of authentication desired, etc. A summary of the technology's authentication capabilities:

- *Inherent/Default* - As users' fingerprints are <u>permanently</u> stored in a PDK Bio Key, most users will inherently want to safeguard their Key and their Key's use. By not doing so they may expose themselves to fraudulent/wrongful use ... and any associated consequences.
- *Newly-acquired Keys* - Prior to being initialized and registered, a PDK Bio Key is functionally-equivalent to any standard (non-bio) PDK Key.
- *BOA* - If a Key has been initialized but not registered, a PDK Bio Key provides the same levels of security as that of any standard (non-bio) PDK Key, and can also optionally guarantee that the owner is (or isn't) the individual attempting to use it.
- *EOA* - If a Key has been initialized and registered, a PDK Bio Key provides the same levels of security as that of any standard (non-bio) PDK Keys, and can also optionally guarantee that: 1) the owner is (or isn't) the individual attempting to use it, 2) the Key has been registered (verifying the Key's owner has been authenticated by a third-party), and 3) the Key's status is valid.

Margent Development, LLC - PDK Bio Key

Origination date: 11-25-04

Basic Use:

Owner Initialization Procedure (OIP)

Prior to using a Bio Key's bio authentication capabilities, an OIP must be successfully completed. Upon a successful OIP completion, a set of bio scans (e.g. fingerprints) is permanently stored within the Key's internal bio database (memory). This permanently-stored data is then available for comparison to bio scans obtained as part of typical/ongoing Key usage. A Key's OIP can only be run one time. A summary of the OIP:

1. The user touches the Bio Reader (or separate button, etc.) in a set manner (such as contacting the Bio Reader for 30 seconds, or tapping 10 times in rapid succession, etc.) indicating they wish to begin the OIP. If the OIP has never before been completed (the Key has not been initialized), the procedure begins.
2. The LED then lights in a certain color (e.g. green), pulses a set number of times, or similar indicating it has entered *initialization* mode.
3. The user now presses a finger to the Bio Reader and holds it there while a scan is performed and validated. The reader may require multiple scans to confirm validity, indicating that need via the LED.
4. Once the LED indicates a valid read is secured, the user can continue the process to obtain additional reads (e.g. of other fingers), with the LED indicating the validity of each. This continues until either all storage locations are filled, or the user wishes to stop (not all locations need to be filled, and multiple locations can temporarily store the same data if desired).
5. When ready, the user touches the Bio Reader (or separate button, etc.) in a set manner indicating scanning is complete. The LED responds by changing states (colors, pulse timing, etc.), signifying the Key is ready to store the bio data. At this point, the user has the option to abort, start over, or continue.
6. The user then touches the Bio Reader (or separate button, etc.) in a set manner indicating the desired action. If they chose to abort or start the process over, the Key clears all data and reverts to an un-initialized state. If they chose to complete the process, data from each unique scan (i.e. if the same print was scanned multiple times, only one instance is recognized) is permanently stored in the Key's internal bio database, where it can never be added-to, deleted, modified, viewed or (externally) read.
7. If needed, a simple tap on the Bio Reader (or separate button, etc.) will reset the Key to its normal *stand-by* mode.

Basic Owner Authentication (BOA) Process

When accepting users' PDK Bio Keys for low to medium-risk transactions (low-value sales, low-risk government or business access, etc.) entities may elect to perform only the BOA process. This efficient and simple process involves comparing bio data (e.g. fingerprints) read from the user at the time of the transaction to the bio data stored in the Key's bio database during the OIP. The results of the comparison determine whether or not the Key is allowed to complete the authentication process. A summary of the BOA process:

- The user begins the process in the same manner they would were they using any standard (non-bio) PDK Key (i.e. they simply approach the desired RDC to be automatically and wirelessly detected).
- Assuming the RDC has been configured to request bio authentication from PDK Keys attempting access, the request is wirelessly communicated to the Key, and the user is notified by means of their Key's LED.
- After noting the request, the user simply places a finger (any finger included in the OIP is acceptable) on the Key's Bio Reader where it is automatically scanned. The read is validated and then compared to each of the permanently stored reads in the bio database until a match is found or the entire database has been checked.
- If a match is found, the Key simply responds to the RDC as would any standard (non-bio) PDK Key. If a match is not found, the Key will not (*can* not) respond, which will appear to the RDC as if no Key was detected. Under either scenario, the RDC will respond according to standard PDK procedures.

NOTE: *Functionally equivalent variations of the above process may exist. For instance, instead of a Key not responding at all when invalid bio scans are obtained, it may respond with an "invalid" message or similar. Regardless of the implementation, the end result is unchanged (the Key will not provide access to the protected item).*

Enhanced Use:

Owner Confirmation Procedure (OCP)
At any time after a Key's OIP has been completed, an OCP can be performed. The OCP provides a means of validating that a specific individual's bio scan is or isn't a match to the bio data stored in a Key's internal bio database during the OIP. The OCP enables a simple means for a third-party witness to authenticate a Key's true owner (the one who actually performed the OIP) prior to formally registering it (see below for details). A summary of the OCP:

1. The user touches the Bio Reader (or separate button, etc.) in a set manner (such as contacting the Bio Reader for 30 seconds, or tapping 10 times in rapid succession, etc.) indicating they wish to begin the OCP.
2. The LED then lights in a certain color (e.g. green), pulses a set number of times, or similar indicating it has entered *confirmation* mode.
3. The user now presses one finger at a time on the Bio Reader, waiting with each for the LED to indicate the Bio Reader has performed a scan, validated the read, and authenticated the data (found a match in the Key's bio database). When a match has been obtained for <u>each</u> of the previously stored reads, the Key's LED indicates the procedure has been successfully completed (and the *user/owner* authenticated). If, in a set period of time a match is not obtained for <u>each</u> read stored during the OIP, the LED will indicate the procedure failed.
4. If needed, a simple tap on the Bio Reader (or separate button, etc.) will reset the Key to its normal *stand-by* mode.

Key Registration (KR) Process
To prepare a Bio Key for use in (optional) high-security transactions (those utilizing EOA) a Bio Key must first be formally registered via the KR process. Registering a Key is to have it recorded in the PDK Central Registry (PCR) - a centralized database controlled by a universally accepted/authorized, unrelated, third-party entity - signifying the Key and owner's authenticity have been verified. The Key's *status* is also maintained in the PCR. A summary of the KR process:

- In the presence of an Authorized Notary/Witness (Witness), the user/owner must successfully perform an OCP. Additionally, the Witness must verify (using methods similar to those used by credit card companies or similar) the owner's identity.
- Upon completion of a successful OCP, and with all relevant data in hand, the Witness records the information below, via the Internet, in a newly-created record within the PCR:
  - Unique Key ID (*as the PCR is aware of <u>every</u> Key ID, this data is automatically/indirectly verified*)
  - Unique Owner ID (typically: name, address, phone #; and possibly: SS#, DOB, etc.)
  - Unique Witness ID (typically: name or ID code # - *which the PCR can optionally verify*)
  - Key Status (In-Service, Out-of-Service, Abandoned, Lost, Stolen, etc.)

  Note: Unless specifically requested by the user/owner, <u>no actual bio data is stored</u>.
- In addition to utilizing the Internet for recording Key registration data, other means - such as sending a notarized (or similar) document to the PCR via US mail, transmitting the information via a personal or automated phone call, etc. - are acceptable.
- Once registered, the valid owner of a particular Key can notify the PCR to report status changes (e.g. the Key is lost or stolen), or to update any other information as needed. Of course, proper owner authentication (similar to that used during the KR process) must occur before such updates can be completed.
- An alternative option for registering Keys - best suited for entities requiring lesser levels/scope of security - is to *privately* register them. The PDK Private Registry (PPR) used for this purpose, is a privately-owned and maintained database, structurally-similar to the PCR database. Entities utilizing Bio Keys in a "closed" environment (where each Key is fully managed, administered, and utilized within the bounds of the entity's purview), may find this to be a preferable option (versus using the PCR). For such entities, an individual(s) from within the organization would likely be defined as the Authorized Notary/Witness.

Enhanced Use (continued):

Enhanced Owner Authentication (EOA) Process
When accepting users' PDK Bio Keys for higher-risk transactions (high-value sales, high-risk government or business access, etc.) entities may elect to perform the EOA process. This process involves completing a standard BOA (the Key's standard internal bio comparison process), then performing a secondary authentication - via the PCR - verifying that the Key was formally registered and its status is currently valid. Note: Users must register their Keys via the KR process prior to attempting to perform an EOA. A summary of the EOA process:

- An RDC must first be configured to operate in EOA mode (typically meaning it is attached to an active Internet portal and software-switched to perform EOAs when needed).
- After completing a successful BOA, the Key's unique ID is electronically transmitted to the PCR for verification.
- The PCR then determines if the Key was ever formally registered, and if so, what its current status is. If validated, the RDC is electronically notified allowing it to complete the transaction in process. If not, any relevant information may (optionally) be transmitted back to the RDC (and receiving party) for use as needed. *Examples include: If the Key was found to have been stolen, the receiving party may wish to take the Key into its possession. If the Key is not yet registered, the user could be informed of the process.*
- While the preferred method of communications between an RDC and the PCR is via the Internet, equivalent (and potentially non-electronic) processes can also be utilized when needed.
- For entities electing to utilize only a PPR, the basic procedures defined above may still be followed ... substituting a PPR for the PCR.