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**

DEFENDANT'S OPENING CLAIM CONSTRUCTION BRIEF

Exhibit 1019
Microsoft v. Proxense
IPR2024-00405

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. ASSERTED PATENTS 1

III. AGREED CLAIM TERMS 2

IV. PERSON OF ORDINARY SKILL IN THE ART 2

V. DISPUTED CLAIM TERMS 3

A. "tamper proof format" ('730 patent claims 1 and 8; '954 patent claim 1) 3

1. The Intrinsic Record Confirms That the Claimed Tamper Proof Format Prevents Any Changes to the Stored Data 4

2. The Extrinsic Evidence Confirms Apple's Construction of "Tamper Proof Format" 6

3. Proxense's Proposed Construction Should Be Rejected 7

B. "access message" ('730 patent claims 1 and 8; '954 patent claim 1) 9

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) 12

1. First Prong of 35 U.S.C. § 112 ¶ 6 Analysis 14

2. Second Prong of 35 U.S.C. § 112 ¶ 6 Analysis 15

VI. CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

Cases

Diebold Nixdorf, Inc. v. Int'l Trade Comm'n,
899 F.3d 1291, 1297 (Fed. Cir. 2018).....14, 15

ePlus, Inc. v. Lawson Software, Inc.,
700 F.3d 509 (Fed. Cir. 2012).....19

Ergo Licensing, LLC v. CareFusion 303, Inc.,
673 F.3d 1361 (Fed. Cir. 2012).....19

Grecia v. Samsung Elecs. Am., Inc.,
780 F. App'x 912 (Fed. Cir. 2019).....17

Proxense, LLC v. Google LLC,
6:23-cv-320-ADA (W.D. Tex. 2023).....1

Proxense, LLC v. Microsoft Corp.,
6:23-cv-319-ADA (W.D. Tex. 2023).....1, 9

Proxense, LLC v. Samsung Electronics Co., Ltd. et al.,
6:21-cv-00210-ADA (W.D. Tex. 2021).....1, 9, 10, 13

Rain Computing, Inc. v. Samsung Elecs. Am., Inc.,
989 F.3d 1002 (Fed. Cir. 2021).....17

Robert Bosch LLC v. Snap-On Inc.,
769 F.3d 1094 (Fed. Cir. 2014).....16, 20

Saffran v. Johnson & Johnson,
712 F.3d 549 (Fed. Cir. 2013).....5

Shire Dev., LLC v. Watson Pharms., Inc.,
787 F.3d 1359 (Fed. Cir. 2015).....5

Synchronoss Techs., Inc. v. Dropbox, Inc.,
987 F.3d 1358 (Fed. Cir. 2021).....19

Trading Techs. Int'l, Inc. v. Open E Cry, LLC,
728 F.3d 1309 (Fed. Cir. 2013).....3

Williamson v. Citrix,
792 F.3d 1339 (Fed. Cir. 2015)..... *passim*

WSOU Invs. LLC v. Google LLC,
2023 U.S. App. LEXIS 25255, 2023 WL 6210607 (Fed. Cir. Sep. 25, 2023) 14, 15

Statutes

35 U.S.C. § 112 13

35 U.S.C. § 112 ¶ 6 ..... *passim*

Other Authorities

Manual of Patent Examination Procedures § 2181 14

TABLE OF EXHIBITS

EXHIBIT NO.	DESCRIPTION
1	Chart Listing the Parties' Agreed Constructions
2	U.S. Patent No. 8,352,730
3	U.S. Patent No. 8,886,954
4	U.S. Patent No. 10,698,989
5	Declaration of Creed Jones, PhD in Support of Defendant's Opening Claim Construction Brief
6	'730 File History Excerpts, July 5, 2011 Amendment
7	'730 File History Excerpts, December 5, 2011 Amendment
8	'954 File History Excerpts, September 13, 2013 Amendment
9	*The Wiley Electrical and Electronics Dictionary* definition entry for "tamper proof" (APL-PROXENSE_01138862)
10	*The Authoritative Dictionary of IEEE Standards Terms* definition entry for "tamper protection" (APL-PROXENSE_01138858)
11	*The American Heritage College Dictionary* definition entry for "tamper proof" (APL-PROXENSE_01138854)
12	September 13, 2024 E-mail Correspondence from Maxim Price
13	Proxense's Identification of Claim Terms
14	'954 File History, April 2, 2014 Amendment
15	Complaint in *Proxense, LLC v. Samsung Electronics, Co., Ltd., et al.*, dated March 5, 2021
16	Complaint in *Proxense, LLC v. Google LLC, et al.*, dated May 2, 2023
17	Complaint in *Proxense, LLC v. Microsoft Corporation*, dated May 2, 2023
18	Claim Construction Order in *Proxense, LLC v. Microsoft Corp*, signed May 24, 2024
19	'730 File History Excerpts, Resp. to November 22, 2010 Office Action
20	'954 File History Excerpts, Resp. to June 13, 2013 Office Action

Defendant Apple Inc. ("Apple") submits this opening claim construction brief related to U.S. Patent Nos. 8,352,730 ("the '730 patent"), 8,886,954 ("the '954 patent"), 10,698,989 ("the '989 patent"), 8,646,042 ("the '042 patent"), and 9,679,289 ("the '289 patent") (collectively, the "asserted patents").

I. INTRODUCTION

The Court has construed certain terms in the claims of the asserted patents in three prior cases, in which Proxense has asserted one or more of the asserted patents against Samsung, Microsoft, and Google, respectively. *See Proxense, LLC v. Samsung Elecs. Co. Ltd.*, 6:21-cv-210-ADA (W.D. Tex. 2021); *Proxense, LLC v. Microsoft Corp.*, 6:23-cv-319-ADA (W.D. Tex. 2023); *Proxense, LLC v. Google LLC*, 6:23-cv-320-ADA (W.D. Tex. 2023). Based upon the Court's prior constructions, the parties have reached agreement on several claim terms. The parties continue to dispute the meaning of three claim terms across the five asserted patents.

The Court construed the term "access message" differently in two prior cases, and the parties dispute which claim construction the Court should adopt here. Apple proposes that the Court adopt its most recent claim construction in the Microsoft case. Ex. 18, *Proxense, LLC v. Microsoft Corp.* 6:23-cv-00319-ADA (W.D. Tex. 2023), Dkt. No. 66 (Claim Construction Order). The Court has not previously construed the other two disputed terms: "tamper proof format" and "verification unit." Apple's construction of "tamper proof format" reflects the term's plain and ordinary meaning in the context of the asserted '730 and '954 patents. "Verification unit" is a means-plus-function limitation and is invalid as indefinite because the specification fails to disclose sufficiently definite structure for the claimed functions.

II. ASSERTED PATENTS

The five patents asserted by Proxense come from two patent families: (1) three "Biometric Authentication Patents," which consist of U.S. Patent Nos. 8,352,730, 8,886,954, and

10,698,989; and (2) two "Hybrid Device Patents," which consist of U.S. Patent Nos. 8,646,042 and 9,679,289. All disputed terms appear in the Biometric Authentication Patent claims. The parties do not dispute the construction of any terms in the Hybrid Device Patent asserted claims.

The Biometric Authentication Patents relate generally to "computerized authentication" using biometric data. Ex. 2 ('730 patent) at 1:15–18; Ex. 3 ('954 patent) at 1:19–22; Ex. 4 ('989 patent) at 1:35-38. The patents generally disclose a distributed form of biometric authentication involving a biometric key that persistently stores biometric data in a tamper-resistant format, a scanner that collects biometric data from a user, and an integrated device that compares the scan against the biometric data and sends a code, for example to an application, to indicate that the user was successfully verified. Ex. 2 ('730 patent) at 1:59-67; Ex. 3 ('954 patent) at 2:4-12; Ex. 4 ('989 patent) at 2:9-20.

III. AGREED CLAIM TERMS

The parties have agreed to constructions for a number of claim terms recited in the asserted claims. Attached as Exhibit 1 is a chart listing the parties' agreed constructions.

IV. PERSON OF ORDINARY SKILL IN THE ART

A person of ordinary skill in the art with respect to the Biometric Authentication patents would have had at least a bachelor's degree in computer or electrical engineering or an equivalent engineering discipline, and at least three years of experience in the field of biometrics, encryption and security, or the equivalent. Additional education could substitute for professional experience, and significant work experience could substitute for formal education. Ex. 5 (Declaration of Dr. Creed Jones in Support of Apple's Opening Claim Construction Brief) ("Jones Decl.") at ¶ 32.

V. DISPUTED CLAIM TERMS

A. "tamper proof format" ('730 patent claims 1 and 8; '954 patent claim 1)

Term and Claims	Apple's Construction	Proxense's Construction
"tamper proof format" '730 patent, claims 1, 8 '954 patent, claim 1	Plain and ordinary meaning, wherein the meaning is "a format that prevents any changes to the stored data"	Plain and ordinary meaning

The '730 and '954 patents are directed to systems and methods for storing biometric data, codes, and other data values in a tamper proof format. These patents are part of the same family, with the '954 patent claiming priority to the '730 patent, and they share much of the same specification including the same relevant disclosures. Because these patents are within the same family, share the same relevant disclosures, and list the same single inventor, the use of the disputed term in each patent and its prosecution history informs the proper construction of the "tamper proof format" term across both patents. *See Trading Techs. Int'l, Inc. v. Open E Cry, LLC*, 728 F.3d 1309, 1323 (Fed. Cir. 2013) ("[P]rosecution history regarding a particular limitation in one patent is presumed to inform the later use of that same limitation in related patents, 'unless otherwise compelled.'").

The dispute regarding "tamper proof format" centers around whether the claimed format of the stored data provides the tamper proofing by preventing the stored data from changing. Apple contends that the specification, the applicant's statements during prosecution, and contemporaneous extrinsic evidence, all support this understanding of the term's plain and ordinary meaning. On the other hand, Proxense offers a plain and ordinary meaning without any clarification or explanation. Proxense appears to advance a much broader meaning divorced from the patent specification and its own statements confirming a more limited understanding of the plain and ordinary meaning here.

1. The Intrinsic Record Confirms That the Claimed Tamper Proof Format Prevents Any Changes to the Stored Data.

The claim language and the specification demonstrate that a "tamper proof format" is one "that prevents any changes to the stored data." Claims 1 and 8 of the '730 patent and claim 1 of the '954 patent each claim storing "biometric data . . . and other data values . . . in a tamper proof format written to a storage element." The plain language of the claims indicates a high degree of resilience or immunity from tampering derived from the format in which the data is stored. The specification disclosures echo this meaning. Both patents explain that the storage itself and the manner in which it stores data provide "a tamper-proof format to prevent changes to the stored data." Ex. 2 ('730 patent) at 4:36-42; Ex. 3 ('954 patent) at 5:29-35. The patents further explain that "[t]amper-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)." *Id.* Apple's construction mirrors the patents' own description where the claimed "format" provides the claimed "tamper proof" feature by preventing changes to the stored data.

The patent applicant's statements during prosecution mirror the narrower meaning espoused in the patent specification. During the '730 patent prosecution, the applicant amended the claims to distinguish the prior art by, among other things, replacing "tamper resistant format" with "tamper proof format." Ex. 6 ('730 File History excerpts, July 5, 2011 Amendment) at 2-3 and 5. In its response to a final rejection, the applicant explicitly rejected the examiner's broader meaning of the term. According to the examiner, the prior art disclosed storing data in a tamper proof format such that the data "cannot be altered" at least because the device that was "highly resistant to reverse engineering, cloning and other techniques for tampering." Ex. 7 ('730 File History excerpts, December 5, 2011 Amendment) at 10. The applicant disagreed and explained

that "'[h]ighly resistant to . . . tampering' is not the same as 'tamper proof' as 'proof' by general definition indicates a greater degree of imperviousness than 'resistant.'" *Id.*; *see also* Ex. 8 ('954 File History excerpts, September 13, 2013 Amendment) at 13-14 (being "'highly resistant to reverse engineering . . . and other techniques for tampering' is not the same as 'tamper proof' as 'proof' by general definition indicates a greater degree or imperviousness than 'resistant.'"). The applicant distinguished other prior art arguing that there was "no disclosure or mention that the biometric information is tamper proof <u>in that the new biometric information cannot be written or that existing biometric information cannot be modified</u>." Ex. 7 ('730 File History excerpts, December 5, 2011 Amendment) at 11.[1] The applicant's statements clearly and unambiguously advocated for a meaning of tamper proof format that requires a format providing a higher degree of protection due to it preventing the creation of new data and modification of existing data. Disclaimers of claim scope in patent prosecution bind Proxense here. *See Saffran v. Johnson & Johnson,* 712 F.3d 549, 559 (Fed. Cir. 2013) (finding binding disclaimer in original prosecution). However, the applicant's statements need not rise to the level of disclaimer or unmistakable disavowal of claim scope in order to inform the Court's claim construction. *See Shire Dev., LLC v. Watson Pharms., Inc*., 787 F.3d 1359, 1366 (Fed. Cir. 2015) (even if "prosecution history statements do not rise to the level of unmistakable disavowal, they do inform the claim construction").

The claim language, the specifications, and the applicant's statements during prosecution confirm the plain meaning of "tamper proof format" reflected in Apple's construction, which is a format that prevents any changes to the stored data.

[1] All emphases in quoted language have been added, unless otherwise indicated.

2. The Extrinsic Evidence Confirms Apple's Construction of "Tamper Proof Format"

The available extrinsic evidence confirms that Apple's construction is correct. For example, dictionaries from the relevant time period demonstrate that the term "tamper proof" indicates a higher degree of protection than "tamper resistant." The *Wiley Electrical and Electronics Dictionary* defines "tamper proof" as "[n]ot allowing, or impervious to tampering" and explains that "[i]t is very difficult to attain such a degree of protection." Ex. 9 at APL-PROXENSE_01138865. The same dictionary also defines the less-stringent "tamper-resistance" as "[t]he property or characteristic of affording a comparatively high degree of protection against tampering." *Id.*

Other contemporaneous dictionaries explain that tamper proofing or tamper protection increases system security by protecting against modification of system resources. For example, *The Authoritative Dictionary of IEEE Standards Terms* defines "tamper protection: as "[t]he aspect of physical security concerned with the protection of system resources from unauthorized modification, especially where modifying or altering a component degrades system security." Ex. 10 at APL-PROXENSE_01138861; *see also* Ex. 11 at APL-PROXENSE_01138857 (defining "tamper proof" as being "[d]esigned to prevent tampering or provide evidence of tampering."). This evidence aligns with the applicant's own statements during patent prosecution that claimed system "is unable to be subsequently altered; thereby beneficially increasing security and eliminating the potential for tampering." Ex. 7 ('730 File History December 5, 2011 Amendment) at 11.

Thus, the patent specifications, the applicant's statements during patent prosecution regarding claim scope, and the extrinsic evidence each uniformly confirm that, in the context of

the ’730 and ’954 patents, the plain and ordinary meaning of “tamper proof format” is “a format that prevents any changes to the stored data.”

3. Proxense’s Proposed Construction Should Be Rejected.

Construction of this claim term is necessary to resolve the parties’ dispute regarding the plain and ordinary meaning of the term. While Proxense contests that Apple’s construction captures the plain and ordinary meaning, the substance of Proxense’s dispute remains unclear. During this case, Proxense stated that it “believe[s] Apple’s proposed construction for ‘tamper proof format’ is accurate but only if the claim terms being construed are the full claim terms ‘tamper proof format… that is unable to be subsequently altered’ and ‘tamper proof format…. that is not capable of being subsequently altered.’” Ex. 12 (9/13/2024 email from Maxim Price) at 1. Thus, rather than articulating any inaccuracy with respect Apple’s proposed construction, Proxense apparently seeks to apply Apple’s proposed construction to a different set of words in the claim.

Proxense’s belated proposal to construe the longer claim phrases should be rejected because it improperly conflates two separate claim requirements.[2] “Tamper proof format” and “unable to be subsequently altered” describe complimentary but distinct requirements of the claims. “Tamper proof format” is a format for storing data that prevents any changes to the stored data, while the “unable to be subsequently altered” language is broader. For example, a Microsoft Word document may be stored in a “locked” format, which prevents changes to the stored data, while still permitting the stored data to be subsequently altered (e.g. by unlocking the

[2] Notably, the longer claim phrases also were not identified by any party as claim terms requiring construction. Although Proxense had an opportunity to identify these claim terms for construction, it chose not to do so. Ex. 13 (Proxense identification of claim terms).

document, changing the data, and relocking the document). The latter limitation would prevent such a scenario.

The prosecution history confirms the separate nature of these terms. During prosecution, the applicant added both limitations to the '730 patent through the same amendment, and the applicant relied on both limitations when distinguishing the prior art. *See* Ex. 6 ('730 File History excerpts, July 5, 2011 Amendment) at 2-3 and 5. The applicant explained that systems that stored data in tamper resistant formats but still allowed for data to be added or modified would not practice the claims. According to the applicant, a system that allows data to be added or modified, even if such actions are rare or not normal, does not equate to being unable to repeat the process, and thus does not satisfy the claim language. Ex. 7 ('730 File History December 5, 2011 Amendment) at 11. Prior art cited by the examiner during prosecution related to use of biometric information for data protection, such as storing a hash of the fingerprint or encrypting the fingerprint. *Id.* However, that prior art also allowed for a switch to "be flipped at any point in time allowing the enrollment of additional or other biometric information." *Id.* at 11-12. The applicant explained that, unlike the prior art, its claimed device "is <u>unable to be subsequently altered</u>, thereby beneficially increasing security and <u>eliminating the potential for tampering</u>." *Id.* at 12; *see also* Ex. 8 ('954 File History, September 13, 2013 Amendment) at 15 (same). Consistent with its statements during prosecution, the applicant included separate terms to ensure that under any scenario, the data is unable to be changed—not only must the data be stored in a "tamper proof format," but the data also must be unable to be subsequently altered (e.g. by flipping a switch to allow modifications to the data as disclosed by the cited prior art. *Id.*; *see also* Ex. 14 ('954 File History, April 2, 2014 Amendment) at 12-13 (providing examples to

distinguish uncommon behavior of a system from a system that is unable or not capable of such behavior).

Therefore, to the extent there remains a substantive dispute as to the meaning of "tamper proof format," the Court should adopt Apple's construction.

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*: A signal or notification enabling or announcing access

The parties dispute which of the Court's prior constructions for this claim term should be adopted in this case. Apple proposes that the Court adopt its most recent construction for this claim term in the *Proxense v. Microsoft* case. Proxense instead proposes that the Court go back in time and adopt its earlier construction in the *Proxense v. Samsung* case—the same construction that Proxense proposed, and the Court correctly rejected, in *Proxense v. Microsoft*.

On March 5, 2021, Proxense filed suit against Samsung asserting that Samsung infringed claims of five patents including two of the Biometric Authentication Patents at issue in this case (the '730 and '954 patents). Ex. 15 (Samsung Complaint). In that case, the Court construed "access message" in claims 1 and 15 of the '740 patent and claim 1 of the '954 patent to mean "a signal or notification enabling or announcing access." *Proxense, LLC v. Samsung Electronics Co., Ltd. et al.,* 6:21-cv-00210-ADA (W.D. Tex. 2021), Dkt. No. 43 (Claim Construction Order).

Following the conclusion of the *Samsung* case, Proxense filed lawsuits against Microsoft and Google asserting one or more of the Biometric Authentication Patents. Ex. 16 (Google Complaint); Ex. 17 (Microsoft Complaint). In *Proxense v. Microsoft*, the parties again disputed the proper claim construction of "access message." Ex. 18, *Proxense LLC v. Microsoft Corp.*,

6:23-cv-00319-ADA (W.D. Tex. 2023), Dkt. No. 66 (Claim Construction Order). Proxense contended that the Court should adopt its prior claim construction from *Proxense v. Samsung*. *Id.* The Court rejected Proxense's proposal, and instead held that the term should be afforded its plain and ordinary meaning. *Id.*

In this case, Proxense does not want to accept the Court's most recent "plain and ordinary meaning" construction of "access message." Proxense instead proposes that the Court adopt its claim construction from *Proxense v. Samsung*, which the Court rejected approximately five months ago. The Court should again reject Proxense's construction, because it is unsupported by the intrinsic record.

First, Proxense's construction conflicts with the surrounding claim language in each asserted claim. Proxense's construction contemplates that an "access message" may either enable or announce access. However, the asserted claims do not support that an "access message" may merely announce access. The term "access message" appears exactly once in each asserted claim, and in each instance, requires that the receipt of the "access message" result in allowing the user access:

- "<u>receiving an access message</u> from the agent <u>allowing the user access</u> to an application" Ex. 2 ('730 patent), claim 1
- "<u>receives an access message</u> from the agent <u>allowing the user access</u> to an application" Ex. 2 ('730 patent), claim 8
- "<u>receiving</u>, at an application, <u>an access message</u> 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 <u>allowing the user access</u> to the application" Ex. 3 ('954 patent), claim 1

Thus, each asserted claim expressly requires that receipt of the "access message" allows the user access to an application. An "access message" that merely announces access would not practice any asserted claim. Put another way, if an "access message" can alternatively enable or announce

access, as Proxense contends, then in instances where it performs the announcing function, the requirement that "receiving […] an access message… allowing the user [access]" would not be satisfied. *See* Ex. 2 ('730 patent), claims 1 and 8; Ex. 3 ('954 patent), claim 1.

Second, Proxense's proposed construction is unsupported by the patent specifications. The terms "notification" and "announcing" (or "announce") are not found in the '730 or '954 patent specifications. *See* Ex. 2 ('730 patent), *passim*; Ex. 3 ('954 patent), *passim*. And, although the word "signal" appears in the specifications, it is not used to describe the "access message."

Nor do the specifications describe the "access message" as merely performing an announcing function. On the contrary, mirroring the asserted claims, the specifications explain that receipt of an access message results in allowing the user access. For example, the Abstract of the '954 patent recites:

> The authentication unit… <u>receives an access message</u> from the agent indicating that the agent successfully authenticated the one or more codes and other data values and <u>allows the user to access</u> an application.

Ex. 3 ('954 patent), Abstract. Similarly, the specifications of both patents explain that if the user is successfully authenticated, an "access message" is sent to allow user access; otherwise, a separate message is sent to deny the user access:

> If the authentication is successful, <u>the trusted key authority sends an access message</u> to the application <u>to allow user access</u> and/or provide additional information from the profile 740 (such as the user's age). If authentication is not successful, authentication fails 750 and the message to the application indicates that the user should be denied access.

Ex. 2 ('730 patent) at 7:18-21; Ex. 3 ('954 patent) at 8:12-17. Notably, this passage contemplates that an "access message" may also, or instead, "provide additional information from the profile 740 (such as the user's age)." However, "providing additional information," does not <u>announce</u> access, as contemplated by Proxense's construction. Rather, this passage simply contemplates

that the "access message" may comprise profile information (such as the user's age), which the application (*e.g.*, slot machine) can use to determine whether or not to grant access. *See, e.g.*, Ex. 2 ('730 patent) at 2:6-14 ("[T]he trusted key authority can store a profile associated with the biometric key having the code. The profile can contain user information such as name, age, account numbers, preferences and the like…The profile can also be sent to the authentication module for use by the application (e.g., an age of user sent to a casino machine."); *id* at 6:32-53 (describing establishment of a profile). In such scenarios, the "access message" does not announce access, but rather provides information for the application to use in determining whether or not to allow the user access.

Third, Proxense's construction finds no support in the prosecution history. Like the claims and specification, the applicant's statements during prosecution of both the '730 and '954 patents confirm that receipt of an "access message" results in allowing the user access. *See* Ex. 19 ('730 File History excerpts, Resp. to November 22, 2010 Office Action) at 8 ("The user is allowed access responsive to receipt of an access message from the agent that authenticates the code."); Ex. 20 ('954 File History excerpts, Resp. to June 13, 2013 Office Action) at 12 ("The user is allowed access responsive to receipt of an access message from the agent that authenticates the code."). The prosecution history lacks any discussion of an "access message," which merely announces access, as contemplated by Proxense's construction.

Because Proxense's construction is unsupported by the intrinsic record, the Court should again reject it.

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 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" ('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.*[3]

The parties dispute two issues with respect to this claim term: (1) whether the term is subject to construction as a means-plus-function limitation under 35 U.S.C. § 112 ¶ 6,[4] and (2) what structure, if any, in the specification corresponds to the claimed function. Apple's proposed construction should be adopted because: (1) the "verification unit" claim term does not recite any structure, let alone sufficiently definite structure, for performing the recited functions, and (2) the specification fails to disclose sufficient corresponding structure for performing each function recited in the claim term.

[3] This claim term was not construed by the Court in *Proxense v. Samsung*. *Proxense LLC v. Samsung Electronics Co., Ltd. et al.,* 6:21-cv-00210-ADA (W.D. Tex. 2021), Dkt. No. 43 (Claim Construction Order).

[4] In view of the filing date of the patent-in-suit, Apple addresses pre-AIA 35 U.S.C. § 112.

1. First Prong of 35 U.S.C. § 112 ¶ 6 Analysis.

This claim limitation is governed by 35 U.S.C. § 112 ¶ 6, because the term "verification unit" is a generic term drafted in purely functional language. While a claim term that does not use the word "means" is presumed not to be a means-plus-function limitation, that presumption is overcome if the claim term either fails to "recite sufficiently definite structure" or recites "function without reciting sufficient structure for performing that function.'" *Williamson v. Citrix*, 792 F.3d 1339, 1349 (Fed. Cir. 2015)). The focus of this inquiry is on the claim language, and the legal standard is whether the words of the claim connote sufficiently definite structure to a person of ordinary skill in the art ("POSITA"). *Id.*. Here, the presumption against means-plus-function treatment is overcome because the "verification unit" term in claim 8 does not recite any structure, let alone sufficiently definite structure.

The word "unit" in the "verification unit…" term is a "nonce word" that does not connote any particular structure, let alone sufficiently definite structure, to a POSITA. Ex. 5 (Jones Decl.) at ¶¶ 40-41. As the Federal Circuit noted in *WSOU Invs. LLC v. Google LLC*, "the term 'unit' in a vacuum, is defined only by the function it performs, much like terms such as 'element' or 'means." 2023 WL 6210607, 2023 U.S. App. LEXIS 25255, at *4 (Fed. Cir. Sep. 25, 2023); *see also Diebold Nixdorf, Inc. v. Int'l Trade Comm'n*, 899 F.3d 1291, 1297 (Fed. Cir. 2018) (concluding that the term "cheque standby unit" is drafted in means-plus-function format); *see also* Manual of Patent Examination Procedures § 2181 (noting that the presumption against means-plus-function treatment "may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term 'means') and identifying 'unit for' as an example of such a "non-structural generic placeholder").

Placing the word "verification" before the word "unit" in claim 8 of the '730 patent cannot exclude the limitation from means-plus-function treatment, because the phrase

"verification unit" has no well understood structural meaning in the art. Ex. 5 (Jones Decl.) at ¶¶ 42-43. The prefix "verification" is itself purely functional language describing the function of the claimed "unit," *i.e.* something that verifies. *Id.*

Similarly, nothing in the surrounding claim language or in the patent specification sheds light on what the "verification unit" is, other than something that verifies. The remainder of the claim limitation simply requires that the "verification unit" be "in communication with the memory" and recites two functions performed by the "verification unit": (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. Ex. 2 ('730 patent) at claim 8; Ex. 5 (Jones Decl.) at ¶¶ 44-49. Notably, the phrase "verification unit" does not appear in the patent specification.

Because the claimed "verification unit" fails to "recite sufficiently definite structure" and recites "function without reciting sufficient structure for performing that function," it is a means-plus-function limitation. *Williamson*, 792 F.3d at 1349; *see also* WSOU, 2023 WL 6210607, at *4; *Diebold,* 899 F.3d at 1297.

2. Second Prong of 35 U.S.C. § 112 ¶ 6 Analysis.

The second step of the means-plus function analysis requires that the Court "determine whether the specification discloses sufficient structure that corresponds to the claimed function." *Williamson*, 792 F.3d at 1351. In making this determination, the Court "must first identify the claimed function." *Id.* "Then, the court must determine what structure, if any, disclosed in the specification corresponds to the claimed function." *Id.* "Where there are multiple claimed functions… the patentee must disclose corresponding structure to perform all of the claimed

functions." *Id.* at 1351-52. A term governed by § 112 ¶ 6 is indefinite if the specification does not disclose sufficient structure corresponding to the recited function. *Robert Bosch LLC v. Snap-On Inc.*, 769 F.3d 1094, 1102 (Fed. Cir. 2014).

Here, claim 8 of the '730 patent recites two functions of the claimed "verification unit": (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. Ex. 2 ('730 patent) at claim 8; Ex. 5 (Jones Decl.) at ¶ 53. Because the patent specification fails to disclose sufficient structure for performing both claimed functions, and the claim is indefinite. *Robert Bosch*, 769 F.3d at 1102.

The '730 patent specification links both claimed functions to elements depicted in Figure 2, reproduced below:

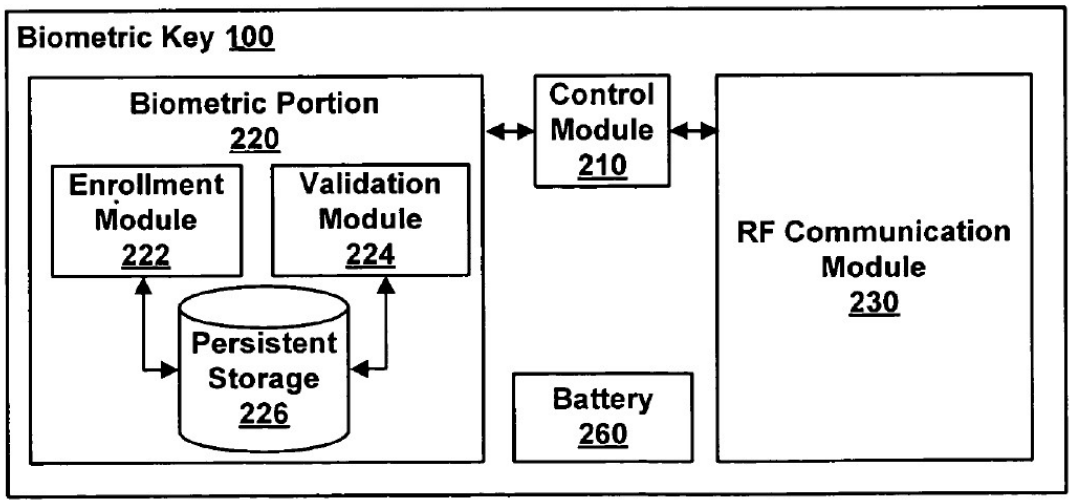


FIG. 2

Ex. 2 ('730 patent) at Fig. 2.

The patent describes the first recited function, "receiv[ing] scan data from a biometric scan for comparison against the biometric data," as being performed by validation module 224. For example, the specification states:

> Validation module 224 can comprise scan pad 120 (FIG. 1) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module 224 determines whether the user's fingerprint matches the stored biometric data from enrollment.

Id. at 4:13-18. Thus, validation module 224 performs the recited function of receiving scan data from a biometric scan (*i.e.* scan data from a user's fingerprint) for comparison against biometric data (*i.e.* the stored biometric data).

Notably, validation module 224 does not connote structure, but rather is itself a purely functional term. Ex. 5 (Jones Decl.) at ¶¶ 57-58. In this regard, the term "'module' is a well-known nonce word that can operate as a substitute for 'means' in the in the context of § 112, para. 6." *Williamson*, 792 F.3d at 1350-51; *see also Rain Computing, Inc. v. Samsung Elecs. Am., Inc.,* 989 F.3d 1002, 1006 (Fed. Cir. 2021) (finding "user identification module" to be a means plus function term); *Grecia v. Samsung Elecs. Am., Inc.*, 780 F. App'x 912, 914-15 (Fed. Cir. 2019) (finding "customization module" to be a means plus function term). Adding the prefix "validation" to the nonce word "module," does not impart a structural meaning to the phrase—rather it simply indicates the function of the "module," *i.e.* validating. Ex. 5 (Jones Decl.) at ¶¶ 57-58.

Although validation module 224 is simply depicted as a black box in Figure 2, the specification describes specific structure for the validation module, *i.e.* "scan pad 120 (Fig. 1) to capture scan data from a user's fingerprint." Ex. 2 ('730 patent) at 4:13-18. The specification further describes the structure of scan pad 120 as follows:

> Scan pad 120 can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad 120 can be sized to fit a thumb or other finger.

Id. at 3:28-30. Because no other structure is disclosed in the specification for performing the first recited function, the structure corresponding to the first recited function is "scan pad 120 (Fig. 1) [configured] to capture scan data from a user's fingerprint." *Id.* at 4:13-18; Ex. 5 (Jones Decl.) at ¶¶ 59-61.

The patent describes the second recited function, "if the scan data matches the biometric data, wirelessly send[ing] one or more codes…," as being performed by control module 210 and RF communication module 230 in Fig. 2 (reproduced above). The specification states:

> Control module 210 coordinates between several functions of biometric key 100. In one embodiment, <u>control module 210 provides a verification code upon successful verification of the user</u>. More specifically, once biometric portion 220 indicates that a fingerprint scan matches biometric data that was collected during enrollment, <u>control module 210 can trigger RF communication module 230 for sending a code indicating that the user was verified</u>.

Ex. 2 ('730 patent) at 3:55-62. Thus, control module 210 and RF communication module 230 together perform the function of "if the scan data matches the biometric data" (*i.e.* the fingerprint scan matches the collected biometric data), "wirelessly sending one or more codes…" (*e.g.* sending a code indicating that the user was verified). Ex. 5 (Jones Decl.) at ¶¶ 62-63.

Like "validation module," neither "control module" nor "RF communication module" connote structure, but rather are purely functional terms. Ex. 5 (Jones Decl.) at ¶¶ 64-65. Both simply recite the "nonce word" module with a prefix that describes the function the module performs, *i.e.* something that performs control or RF communication functions, respectively. *Id.*; *Williamson*, 792 F.3d at 1350-51.

Although the specification describes structure for RF communication module 230, it discloses no structure for control module 210. Specifically, the specification explains that

"[r]adio frequency (RF) communication module 230 is, for example, a transceiver or other mechanism for wireless communication." Ex. 2 ('730 patent) at 4:56-58; Ex. 5 (Jones Decl.) at ¶ 66. However, control module 210 is simply depicted in Fig. 2 as a black box for performing control functions, with no description of structure to implement these control functions in the specification. *Id.* at ¶ 67. The specification makes clear that control module 210 is not a structural component, but rather "merely a grouping of control functions":

> Note that control module 210 of FIG. 2 is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key 100.

Ex. 2 ('730 patent) at 3:66-4:3. The specification includes no description of any structure for performing the described functions. Ex. 5 (Jones Decl.) at ¶¶ 67-68. Rather, the specification includes only a black box illustration of control module 210 with purely functional descriptions of its operation. *Id.*

It is well settled that a "black box" illustration cannot provide sufficient structural disclosure for a term governed by 35 U.S.C. § 112 ¶ 6. *See ePlus, Inc. v. Lawson Software, Inc.*, 700 F.3d 509, 518 (Fed. Cir. 2012)*; see also Ergo Licensing, LLC v. CareFusion 303, Inc.*, 673 F.3d 1361, 1363-64 (Fed. Cir. 2012); *Blackboard, Inc. v. Desire2Learn, Inc*., 574 F.3d 1371, 1383-86 (Fed. Cir. 2009). "Where there are multiple claimed functions… the patentee must disclose corresponding structure to perform all of the claimed functions." *Williamson*, 792 F.3d at 1351-52. Here, the specification clearly links "control module 210" to performing part of the second recited function but fails to disclose adequate structure for a POSITA to recognize and associate with the corresponding function in the claim. *See, e.g.*, *Synchronoss Techs., Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1367 (Fed. Cir. 2021); Ex. 5 (Jones Decl.) at ¶ 69.

Because the "verification unit" limitation is purely functional and the specification fails

to disclose sufficient structure linked to each of its recited functions, claim 8 is indefinite and therefore invalid. *See Robert Bosch*, 769 F.3d at 1102.

VI. CONCLUSION

For the foregoing reasons, Apple respectfully asks the Court to adopt its proposed constructions.

Dated: November 5, 2024

Respectfully submitted,

John M. Guaragna

John M. Guaragna
Texas Bar No 24043308
Michael Saulnier
Texas Bar No. 24131647
DLA PIPER LLP (US)
303 Colorado, Suite 3000
Austin, TX 78701
Tel: (512) 457-7125
Fax: (512) 457-7001
john.guaragna@us.dlapiper.com
michael.saulnier@us.dlapiper.com

Sean Cunningham (*pro hac vice*)
Erin Gibson (*pro hac vice*)
Robert Williams (*pro hac vice*)
Peter Maggiore (*pro hac vice*)
DLA PIPER LLP (US)
4365 Executive Drive, Suite 1100
San Diego, CA 92121
Tel: (858) 677-1400
Fax: (858) 677-1401
sean.cunningham@us.dlapiper.com
erin.gibson@us.dlapiper.com
robert.williams@us.dlapiper.com
peter.maggiore@us.dlapiper.com

Nandan R. Padmanabhan (*pro hac vice*)
Benjamin Yaghoubian (*pro hac vice*)
Martin M. Ellison (*pro hac vice*)
DLA PIPER LLP (US)
2000 Avenue of the Stars
Suite 400, North Tower
Los Angeles, CA 90067

Tel: (310) 595-3000
Fax: (310) 595-3300
nandan.padmanabhan@us.dlapiper.com
benjamin.yaghoubian@us.dlapiper.com
martin.ellison@us.dlapiper.com

Jessica Hannah (*pro hac vice*)
DLA PIPER LLP (US)
555 Mission Street, Suite 2400
San Francisco, CA 94105
Tel: (415) 836-2500
Fax: (415) 659-7370
jessica.hannah@us.dlapiper.com

Ahimsa E. Hodari
Texas Bar No. 24132415
DLA PIPER LLP (US)
845 Texas Avenue, Suite 3800
Houston, TX 77002
Tel: (713) 425-8400
Fax: (713) 425-8401
ahimsa.hodari@us.dlapiper.com

ATTORNEYS FOR DEFENDANT APPLE INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the above and foregoing document has been served on November 5, 2024, to all counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system per Local Rule CV-5. Any other counsel of record will be served by a facsimile and/or first-class mail.

/s/ John M. Guaragna
John M. Guaragna

EXHIBIT 1

Exhibit 1 – Undisputed Terms

The parties have agreed to the following constructions:

8,352,730; 8,886,954; 10,698,989 Patents		
Patent Claims	**Terms, Phrases or Clauses**	**Agreed Construction**
’730 claims 1, 8 ’954 patent, claim 1	“persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value … to a storage element” / “stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value … to the memory”	Plain and ordinary meaning, wherein the meaning is “persistently storing biometric data of the user and a plurality of codes and other data values to a storage element; within this storage element is also (1) a device ID code uniquely identifying the integrated device and (2) a secret decryption value” / Plain and ordinary meaning, wherein the meaning is “stores biometric data of the user and a plurality of codes and other data values to a memory; within this memory is also (1) a device ID code uniquely identifying the integrated device and (2) a secret decryption value”
’730 claims 1, 8 ’954 claim 1 ’989 claim 1	“device ID code” / “ID code” / “identification (ID) code”	A unique code identifying a device

8,6,46,042; 9,679,289 Patents		
Patent Claims	**Terms, Phrases or Clauses**	**Agreed Construction**
’042 patent claims 1, 6 ’289 patent claims 1, 11	“hybrid device”	a device comprising an integrated personal digital key (PDK)[1] and an integrated receiver-decoder circuit (RDC)[2] [1] Wherein “personal digital key (PDK)” is construed as set forth below, i.e., “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user” [2] Wherein “receiver-decoder circuit (RDC)” is construed as set forth below, i.e., “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing”
’042 patent claim 1 ’289 patent claim 1	“A hybrid device comprising”	The preamble of claim 1 of the ’042 patent is limiting. / The preamble of claim 1 of the ’289 patent is limiting.
’042 patent claims 1, 6 ’289 patent claims 1, 11	“personal digital key (PDK)”	an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user

8,6,46,042; 9,679,289 Patents		
Patent Claims	**Terms, Phrases or Clauses**	**Agreed Construction**
’042 patent claims 1, 6 ’289 patent claims 1, 11	“receiver-decoder circuit (RDC)” “reader-decoder circuit (RDC)”	a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing

EXHIBIT 2

US008352730B2

(12) **United States Patent**
Giobbi

(10) **Patent No.: US 8,352,730 B2**
(45) **Date of Patent: Jan. 8, 2013**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(75) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 938 days.

(21) Appl. No.: **11/314,199**

(22) Filed: **Dec. 20, 2005**

(65) **Prior Publication Data**

US 2006/0143441 A1 Jun. 29, 2006

Related U.S. Application Data

(60) Provisional application No. 60/637,538, filed on Dec. 20, 2004, provisional application No. 60/652,765, filed on Feb. 14, 2005.

(51) **Int. Cl.**
G06G 21/00 (2006.01)

(52) **U.S. Cl.** **713/155**; 713/182; 713/186

(58) **Field of Classification Search** 380/23; 713/155, 159, 176, 186; 726/27–30; 382/115; 340/5.52–5.53

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,759,060	A	7/1988	Hayashi et al.
4,993,068	A	2/1991	Piosenka et al.
5,187,352	A	2/1993	Blair et al.
5,296,641	A	3/1994	Stelzel
5,392,433	A	2/1995	Hammersley et al.
5,416,780	A	5/1995	Patel
5,422,632	A	6/1995	Bucholtz et al.
5,450,489	A	9/1995	Ostrover et al.
5,619,251	A	4/1997	Kuroiwa et al.
5,629,980	A	5/1997	Stefik et al.
5,644,354	A	7/1997	Thompson et al.
5,666,412	A	9/1997	Handelman et al.

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 00/62505 A1 10/2000

(Continued)

OTHER PUBLICATIONS

"Alliance Activities: Publications: Identity—Smart Card Alliance," Smart Card Alliance, 1997-2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.smartcardalliance.org/pages/publications-identity>.

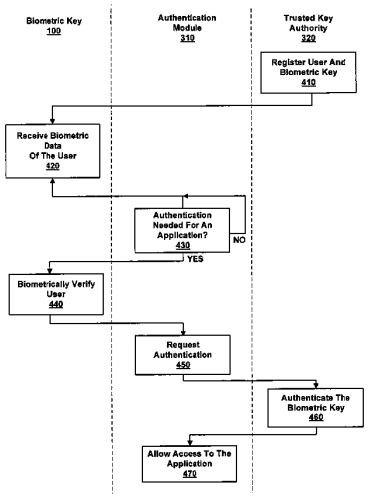
(Continued)

Primary Examiner — Matthew Smithers
Assistant Examiner — Phy Anh Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods are provided for an integrated device that persistently (or permanently) stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a finger-print) can be compared against the biometric data. Once the user has been verified by the integrated device, a code can be wirelessly transmitted for authentication. The authentication module sends the code to a trusted key authority. The trusted key authority checks a list of enrolled integrated devices for a match. If there is a match, the authentication module sends a message to an application to allow access by the user. The trusted key authority also stores a profile associated with the code. The profile can contain user information such as name, age, account numbers, preferences, etc. and can also describe the status of the integrated device.

17 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

5,784,464 A 7/1998 Akiyama et al.
5,825,876 A 10/1998 Peterson, Jr.
5,857,020 A 1/1999 Peterson, Jr.
5,892,825 A 4/1999 Mages et al.
5,894,551 A 4/1999 Huggins et al.
5,898,880 A 4/1999 Ryu
5,917,913 A 6/1999 Wang
5,928,327 A 7/1999 Wang et al.
5,991,399 A 11/1999 Graunke et al.
5,991,749 A 11/1999 Morril, Jr.
6,016,476 A 1/2000 Maes et al.
6,018,739 A 1/2000 McCoy et al.
6,035,038 A 3/2000 Campinos et al.
6,035,329 A 3/2000 Mages et al.
6,038,334 A 3/2000 Hamid
6,041,410 A * 3/2000 Hsu et al. 713/186
6,042,006 A 3/2000 Van Tilburg et al.
6,055,314 A 4/2000 Spies et al.
6,070,796 A 6/2000 Sirbu
6,088,730 A 7/2000 Kato et al.
6,104,334 A 8/2000 Allport
6,121,544 A 9/2000 Petsinger
6,148,142 A 11/2000 Anderson
6,161,179 A 12/2000 Seidel
6,185,316 B1 2/2001 Buffam
6,209,089 B1 3/2001 Selitrennikoff et al.
6,219,109 B1 4/2001 Raynesford et al.
6,219,439 B1 4/2001 Burger
6,247,130 B1 6/2001 Fritsch
6,256,737 B1 7/2001 Bianco et al.
6,266,415 B1 7/2001 Campinos et al.
6,295,057 B1 9/2001 Rosin et al.
6,336,121 B1 1/2002 Lyson et al.
6,336,142 B1 1/2002 Kato et al.
6,363,485 B1 3/2002 Adams et al.
6,367,019 B1 4/2002 Ansell et al.
6,381,747 B1 4/2002 Wonfor et al.
6,385,596 B1 5/2002 Wiser et al.
6,392,664 B1 5/2002 White et al.
6,397,387 B1 5/2002 Rosin et al.
6,401,059 B1 6/2002 Shen et al.
6,411,307 B1 6/2002 Rosin et al.
6,424,715 B1 7/2002 Saito
6,425,084 B1 7/2002 Rallis et al.
6,434,535 B1 8/2002 Kupka et al.
6,446,130 B1 9/2002 Grapes
6,463,534 B1 10/2002 Geiger et al.
6,480,188 B1 11/2002 Horsley
6,490,443 B1 12/2002 Freeny, Jr.
6,510,350 B1 1/2003 Steen et al.
6,523,113 B1 2/2003 Wehrenberg
6,529,949 B1 3/2003 Getsin et al.
6,546,418 B2 4/2003 Schena et al.
6,550,011 B1 4/2003 Sims, III
6,563,805 B1 5/2003 Ma et al.
6,564,380 B1 5/2003 Murphy
6,628,302 B2 9/2003 White et al.
6,632,992 B2 10/2003 Hasegawa
6,647,417 B1 11/2003 Hunter et al.
6,667,684 B1 12/2003 Waggamon et al.
6,683,954 B1 1/2004 Searle
6,697,944 B1 2/2004 Jones et al.
6,709,333 B1 3/2004 Bradford et al.
6,711,464 B1 3/2004 Yap et al.
6,775,655 B1 8/2004 Peinado et al.
6,804,825 B1 10/2004 White et al.
6,806,887 B2 10/2004 Chernock et al.
6,850,147 B2 2/2005 Prokoski et al.
6,873,975 B1 3/2005 Hatakeyama et al.
6,950,941 B1 9/2005 Lee et al.
6,973,576 B2 12/2005 Giobbi
6,975,202 B1 12/2005 Rodriguez et al.
6,983,882 B2 1/2006 Cassone
7,012,503 B2 3/2006 Nielsen
7,090,126 B2 8/2006 Kelly et al.
7,112,138 B2 9/2006 Hedrick et al.
7,137,012 B1 11/2006 Kamibayashi et al.
7,191,466 B1 3/2007 Hamid et al.
7,218,944 B2 5/2007 Cromer et al.
7,249,177 B1 7/2007 Miller
7,305,560 B2 12/2007 Giobbi
7,529,944 B2 5/2009 Hamid
7,574,734 B2 8/2009 Fedronic et al.
7,644,443 B2 1/2010 Matsuyama et al.
7,715,593 B1 5/2010 Adams et al.
7,883,417 B2 2/2011 Bruzzese et al.
2001/0044337 A1 11/2001 Rowe et al.
2002/0007456 A1 1/2002 Peinado et al.
2002/0013772 A1 1/2002 Peinado
2002/0014954 A1 2/2002 Fitzgibbon et al.
2002/0015494 A1 2/2002 Nagai et al.
2002/0023032 A1 2/2002 Pearson et al.
2002/0026424 A1 2/2002 Akashi
2002/0073042 A1 6/2002 Maritzen et al.
2002/0098888 A1 7/2002 Rowe et al.
2002/0103027 A1 8/2002 Rowe et al.
2002/0104006 A1 8/2002 Boate et al.
2002/0109580 A1 8/2002 Shreve et al.
2002/1010804 8/2002 Xu et al.
2002/0138767 A1 9/2002 Hamid et al.
2002/0140542 A1 10/2002 Prokoski et al.
2002/0144117 A1 10/2002 Faigle
2002/0150282 A1 * 10/2002 Kinsella 382/124
2002/0158750 A1 10/2002 Almalik
2002/0178063 A1 11/2002 Gravelle et al.
2002/0191816 A1 12/2002 Maritzen et al.
2003/0036425 A1 2/2003 Kaminkow et al.
2003/0046552 A1 3/2003 Hamid
2003/0054868 A1 3/2003 Paulsen et al.
2003/0054881 A1 3/2003 Hedrick et al.
2003/0055689 A1 3/2003 Block et al.
2003/0079133 A1 4/2003 Breiter et al.
2003/0127511 A1 7/2003 Kelly et al.
2003/0139190 A1 7/2003 Steelberg et al.
2003/0172037 A1 9/2003 Jung et al.
2003/0176218 A1 9/2003 LeMay et al.
2003/0186739 A1 10/2003 Paulsen et al.
2004/0127277 A1 7/2004 Walker et al.
2004/0129787 A1 * 7/2004 Saito et al. 235/492
2004/0209690 A1 10/2004 Bruzzese et al.
2004/0209692 A1 10/2004 Schober et al.
2004/0215615 A1 10/2004 Larsson et al.
2004/0230488 A1 * 11/2004 Beenau 705/18
2005/0074126 A1 * 4/2005 Stanko 380/279
2005/0229007 A1 10/2005 Bolle et al.
2005/0251688 A1 11/2005 Nanavati et al.
2006/0022046 A1 2/2006 Iwamura
2007/0220272 A1 * 9/2007 Campisi et al. 713/186
2008/0188308 A1 8/2008 Shepherd et al.
2009/0328182 A1 12/2009 Malakapalli et al.
2010/0117794 A1 5/2010 Adams
2011/0126188 A1 5/2011 Bernstein et al.

FOREIGN PATENT DOCUMENTS

WO WO 01/22724 A1 3/2001
WO WO 01/75876 A1 10/2001
WO WO 01/77790 A1 10/2001
WO WO 2005/050450 A1 6/2005
WO WO 2005/086802 A2 9/2005

OTHER PUBLICATIONS

"Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002 [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.securitymagazine.com/CDA/Articles/Technologies/3ae610eaa34d8010VgnVCM100000f932a8c0__>.

"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.biopay.com/faqs-lowes.asp>.

Mciver, R. et al., "Identification and Verification Working Together," Bioscrypt™, Aug. 27, 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification% 20Working%20Together.pdf>.

Nilsson, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7,

2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>.
Nordin, B., "Match-On-Card Technology," Precise™ Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf>.
"SAFModule™: A Look Into Strong Authentication," saflink Corporation, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod _WP.pdf>.
"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf>.
Wade, W., "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, Apr. 21, 2003, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet<URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>.
Antonoff, Michael, "Visiting Video Valley," Sound & Vision, pp. 116 and 118-119, Nov. 2001.
Article, "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, Jul. 25, 2000.
Article, "Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, Aug. 14, 2000.
Blum, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, (Oct. 2000), 24-27.
Debow, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p10, Nov. 1989.
Dennis, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, Dec. 2, 1999, 2 pages.
Fasca, Chad, "The Circuit," Electronic News, 45(45) (Nov. 8, 1999), 20.
Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, Jan. 18, 1996.
Lake, Matt, "Downloading for Dollars," Sound & Vision, (Nov. 2000), 137-138.
Lewis, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, Nov. 16, 1995.
Notification of the International Search Report and Written Opinion, PCT/US04/38124, Apr. 7, 2005, 10 pages.
Paget, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, (Dec. 1999), 4 pgs.
Press Release, "Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, Jan. 8, 2002.
Press Release, "Content Protection Plan Targets Wireless Home Networks," www.eetimes.com, Jan. 11, 2002.
Press Release, "Thompson Bets on Smart Cards for Video Encryption," www.informationweek.com, Jun. 7, 2001.
Press Release, "Thompson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001.
"Say Hello to Bluetooth," Bluetooth Web site, 4 pages.
Sapsford, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, (Aug. 14, 2000), B1.
Van Winkle, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, (Jan. 2000), 148-153.
Wallace, Bob, "The Internet Unplugged," InformationWeek, 765(22), (Dec. 13, 1999), 22-24.
Weber, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, (Jul. 24, 2000), B1.
PCT International Search Report and Written Opinion, PCT/US05/43447, Feb. 22, 2007, 7 pages.
PCT International Search Report and Written Opinion, PCT/US05/46843, Mar. 1, 2007, 10 pages.
Non-Final Office Action, U.S. Appl. No. 11/292,330, Dated: Sep. 16, 2010, 23 pages.
United States Office Action, U.S. Appl. No. 11,744,831, Sep. 3, 2010, 27 pages.
International Search Report, PCT/U507/11103, Apr. 23, 2008, 9 pages.
International Search Report, PCT/US07/11104, Jun. 26, 2008, 9 pages.
International Search Report, PCT/US07/11102, Oct. 3, 2008, 11 pages.
International Search Report, PCT/US07/11105, Oct. 20, 2008, 10 pages.
"What is a File?", Apr. 30, 1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed Mar. 11, 2010 via http://waybackmachine.org/1 9980615000000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html.
United States Office Action, U.S. Appl. No. 11/292,330, Dec. 2, 2011, 25 pages.
United States Office Action, U.S. Appl. No. 11/744,831, Dec. 16, 2011, 38 pages.
United States Office Action, U.S. Appl. No. 11/744,832, Feb. 7, 2012, 32 pages.
United States Office Action, U.S. Appl. No. 11/745,249, Feb. 2, 2012, 36 pages.
United States Office Action, U.S. Appl. No. 11/292,330, Apr. 6, 2012, 22 pages.
Pope, Oasis Digital Signature Services: Digital Signing without the Headaches, Internet Computing-IEEE, vol. 10, 2006, pp. 81-84.

* cited by examiner

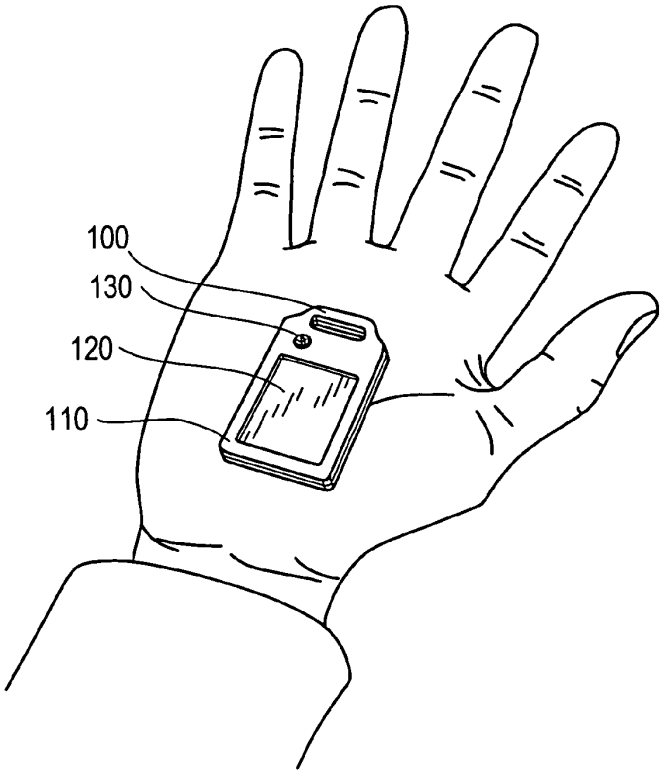

100
130
120
110

FIG. 1

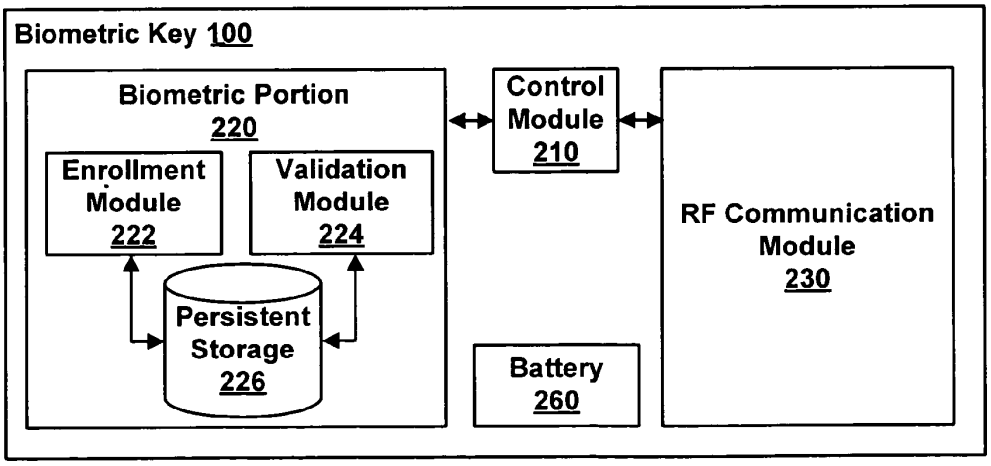

Biometric Key 100
Biometric Portion 220
Enrollment Module 222
Validation Module 224
Persistent Storage 226
Control Module 210
Battery 260
RF Communication Module 230

FIG. 2

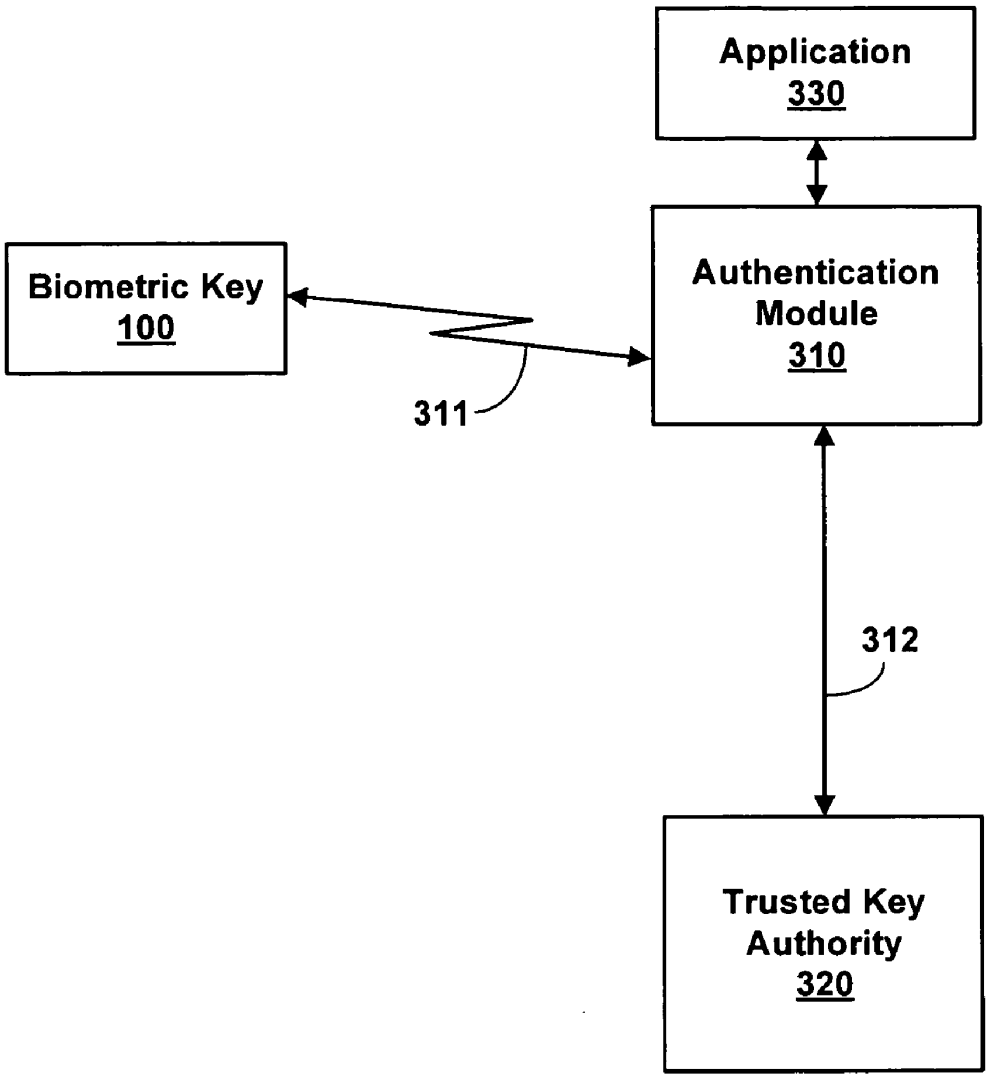

Application
330
Biometric Key
100
Authentication
Module
310
311
312
Trusted Key
Authority
320

FIG. 3

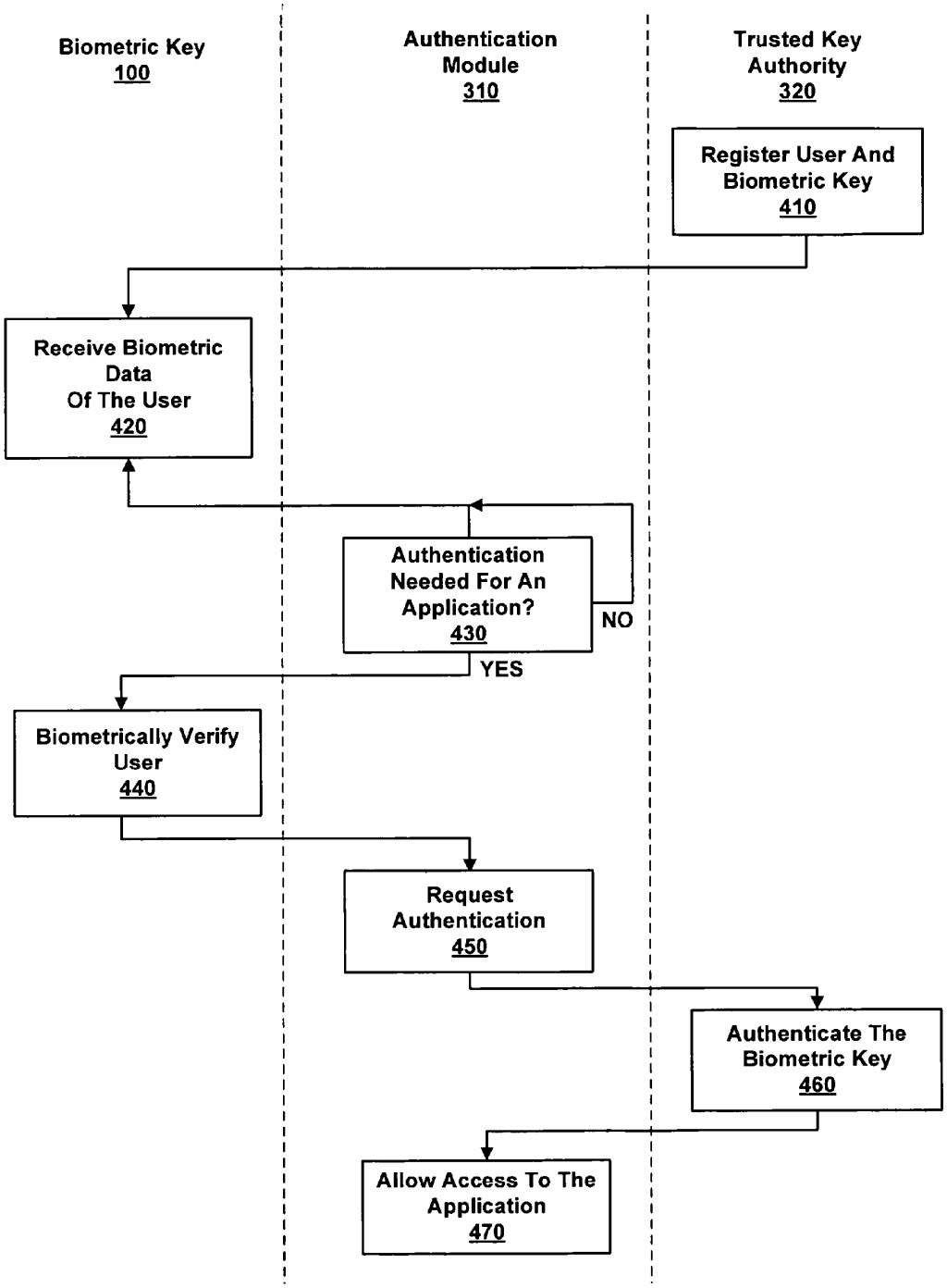

Biometric Key
100
Authentication Module
310
Trusted Key Authority
320
Register User And Biometric Key
410
Receive Biometric Data Of The User
420
Authentication Needed For An Application?
430
NO
YES
Biometrically Verify User
440
Request Authentication
450
Authenticate The Biometric Key
460
Allow Access To The Application
470

FIG. 4

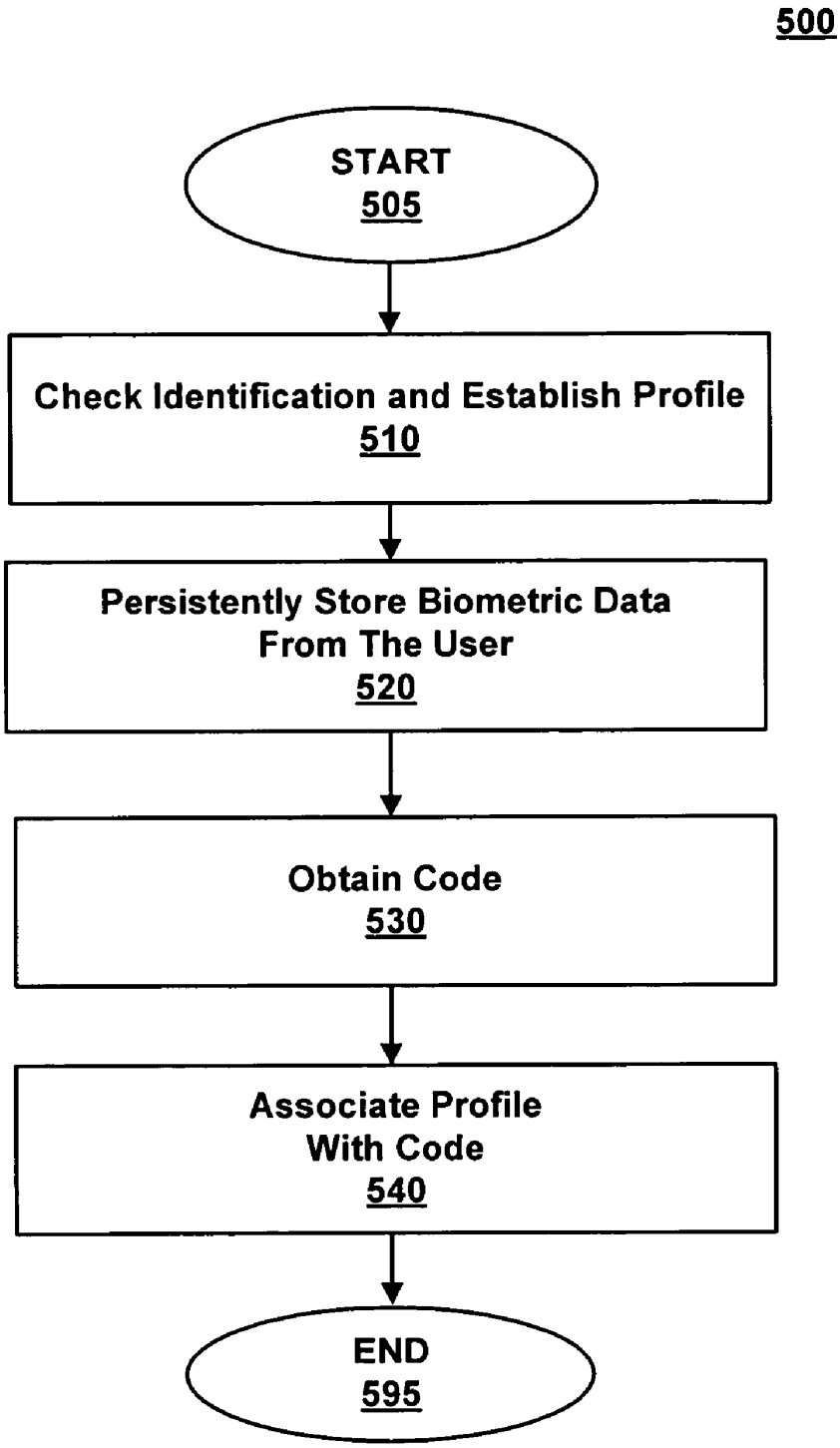

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data
From The User
520
Obtain Code
530
Associate Profile
With Code
540
END
595

FIG. 5

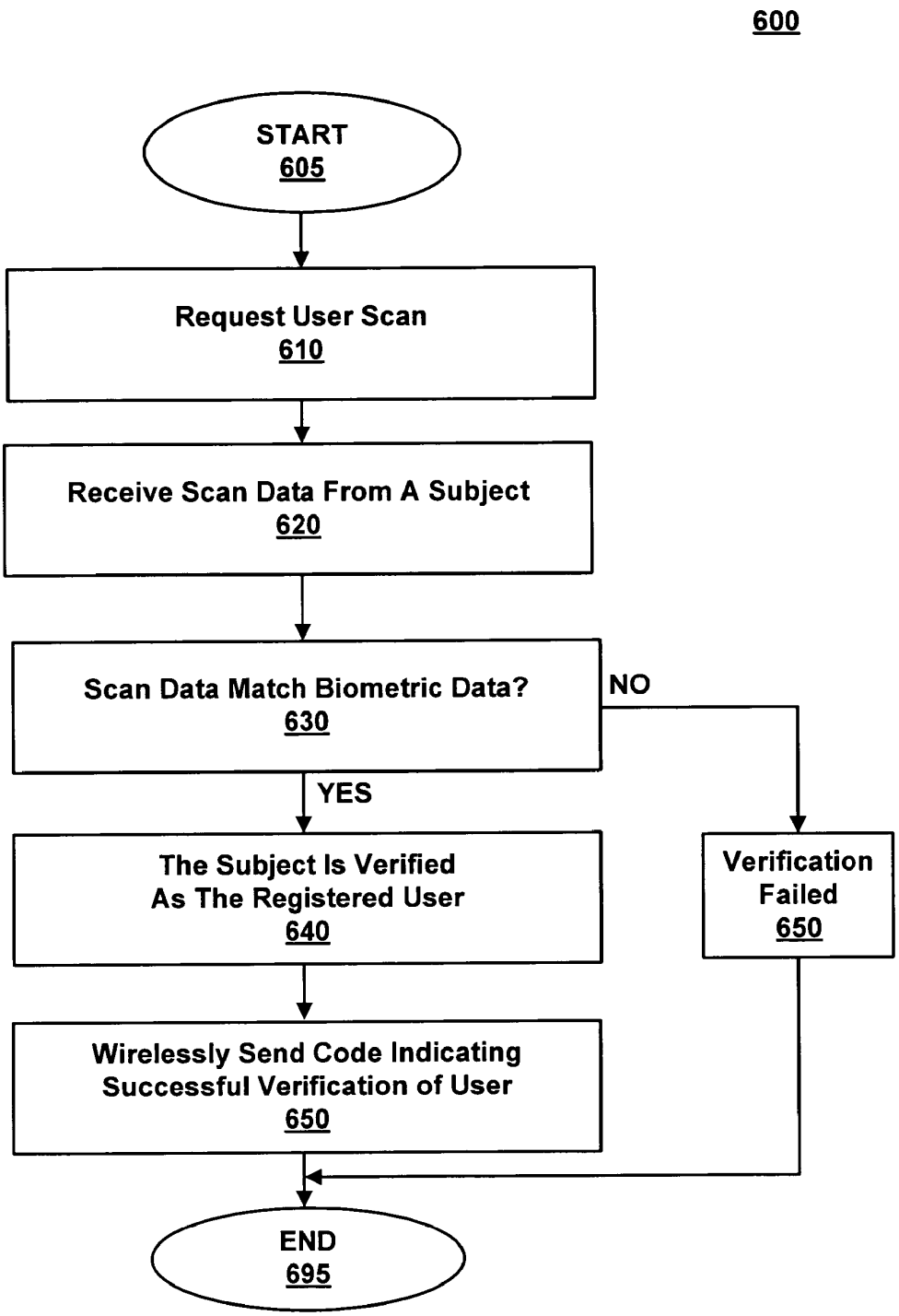

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

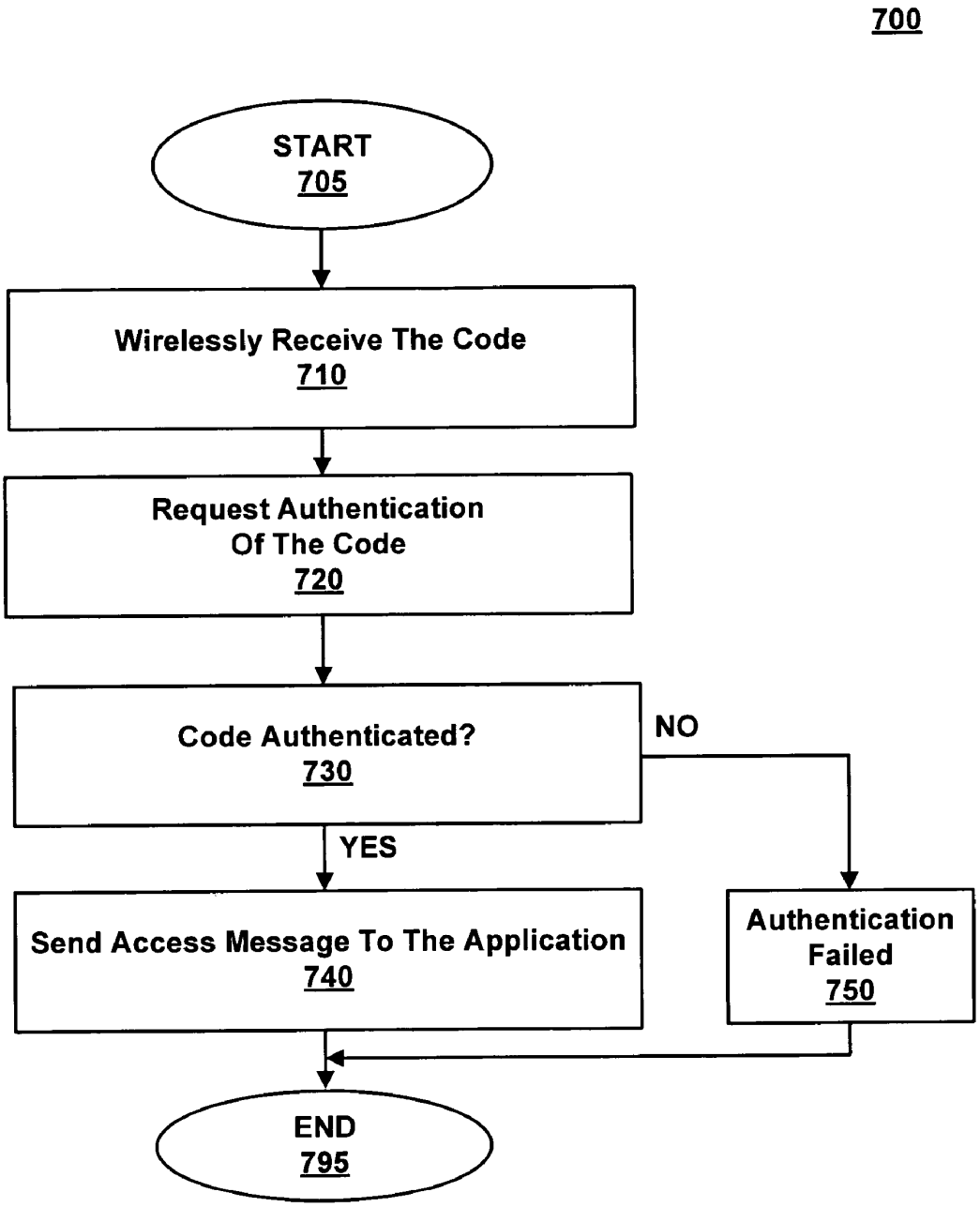

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims the benefit of U.S. Provisional Application No. 60/637,538, filed on Dec. 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on Feb. 14, 2005, the entire contents of both applications being herein incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allowing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A user often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, a biometric key persistently (or permanently) stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a fingerprint or retinal scan) can be compared against the biometric data. Once the user has been verified by the integrated device, the code can be wirelessly transmitted to indicate that the user has been successfully verified.

In one embodiment, an authentication module sends the code to a trusted key authority. The trusted key authority checks a list of enrolled biometric keys to determine whether the code is valid. If the code is valid, the authentication module allows the user to access an application.

In another embodiment, the trusted key authority can store a profile associated with the biometric key having the code. The profile can contain user information such as name, age, account numbers, preferences, and the like. In addition, the profile can describe the status of the key, identify the trusted key authority, and/or contain other information. The profile can also be sent to the authentication module for use by the application (e.g., an age of user sent to a casino machine).

Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in a single key. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the key can be authenticated for an application that is open to the public (i.e., in an open loop system).

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

FIG. **1** is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

FIG. **2** is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

FIG. **3** is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

FIG. **4** is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

FIG. **5** is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

FIG. **6** is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

FIG. **7** is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a finger-print of a subject can be compared against previously-recorded biometric data for

verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

FIG. **1** is a schematic diagram illustrating an example of a biometric key **100** for providing authentication information for a biometrically verified user according to one embodiment of the present invention. Biometric key **100** comprise a frame **110**, a scan pad **120**, and an LED **130**. In one embodiment, biometric key **100** has a small form factor (e.g., the size of a automobile remote control) such that it can be unobtrusively carried by a user.

Frame **110** can be formed by plastic, metal or another suitable material. Frame **110** is shaped to secure scan pad **120**, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame **110** is formed from a unitary molding to protect biometric data. Accordingly, frame **110** cannot be opened to expose the underlying components unless it is broken.

Scan pad **120** can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad **120** can be sized to fit a thumb or other finger. Biometric key **100** of the present embodiment includes LED **130** that lights up to request a fingerprint scan from a user. In one embodiment, LED **130** can also confirm that user verification and/or authentication has completed.

Biometric key **100** can authenticate a user for various purposes. For example, biometric key **100** can allow keyless entry into homes and autos. In another example, biometric key **100** can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key **100** can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key **100** operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

FIG. **2** is a block diagram illustrating biometric key **100** according to one embodiment of the present invention. Biometric key **100** comprises control module **210**, biometric portion **220**, RF communication module **230**, persistent storage **226**, and battery **250**. Biometric key **100** can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key **100** comprises a modified key fob.

Control module **210** coordinates between several functions of biometric key **100**. In one embodiment, control module **210** provides a verification code upon successful verification of the user. More specifically, once biometric portion **220** indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module **210** can trigger RF communication module **230** for sending a code indicating that the user was verified. In another embodiment, control module **210** can work in the opposite direction by detecting a request for verification from RF communication module **230**, and then requesting verification of the user from biometric portion **220**. Note that control module **210** of FIG. **2** is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key **100**.

Biometric portion **220** comprises enrollment module **222**, validation module **224**, and biometric data base **226**. In one embodiment, enrollment module **222** registers a user with biometric key **100** by persistently storing biometric data associated with the user. Further, enrollment module **222** registers biometric key **100** with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key **100** to be stored therein.

Validation module **224** can comprise scan pad **120** (FIG. **1**) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module **224** determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module **224** can send comparison results to control module **210**.

In other embodiments, validation module **224** can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.

Persistent storage **226** persistently stores biometric data from one or more users which can be provided according to specific implementations. 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** can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. 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.

In one embodiment, persistent storage **226** also stores the code that is provided by the key **100** responsive to successful verification of the user. As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key **100**. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments persistent storage **226** stores other data utilized during the operation of biometric key **100**. For example, persistent storage **226** can store encryption/decryption keys utilized to establish secure communications links.

Radio frequency (RF) communication module **230** is, for example, a transceiver or other mechanism for wireless communication. RF communication module **230** can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication **230** can be optimized for low-power usage by, for example, using short-range transceivers. RF communication module **230** can actively send out connection requests, or passively detect connection requests.

Battery **260** can be a conventional power source suitable for the components of biometric key **100**. Battery **260** can be either replaceable or rechargeable. Alternatively, battery **260**

can be embedded within key **100** such that the key must be discarded or recycled upon expiration of the battery.

FIG. **3** is a block diagram illustrating a system **300** for providing authentication information for a biometrically verified user. System **300** comprises an authentication module **310** in communication with biometric key **100**, a trusted key authority **320**, and an application **330**.

Authentication module **310** is coupled in communication with biometric key via line **311** (i.e., a wireless medium such as EM signals), and with trusted key authority **320** via line **312** (e.g., a secure data network such as the Internet, or a cell network). Authentication module **310** can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module **310** serves as a gatekeeper to application **330** by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module **310** provides the code to trusted key authority **320** in order to verify that it belongs to a legitimate key (e.g., when application **330** is security-critical). 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**.

Application **330** is a resource that can be accessed by a verified and authenticated user. Application **330** can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, and the like. Application **330** can execute on the same system as authentication module **310** or on another system in communication with the system of the authentication module. In one embodiment, application module **330** allows access by a user after receiving a message from authentication module **310**. At that point, application **330** can allow direct use by the user, or require that communications continue to pass through authentication module **310** for continued authentication.

Trusted key authority **320** is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, trusted key authority **320** verifies that a code from a biometric key is legitimate. To do so, the trusted key authority **320** stores a list of codes for legitimate biometric keys. The list can be batched or updated each time a new user/key is enrolled. In one embodiment, trusted key authority **320** can also store a profile associated with a biometric key. The profile describes the user associated with the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority **320** is provided by a server or other computerized device.

In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority **320** provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority **320** can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

FIG. **4** is a flow chart illustrating a method **400** for authenticating a biometrically verified user using a trusted key authority (e.g., authority **320**). A biometric key (e.g., biometric key **100**) is registered **410** with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled **420** with the biometric key as described below with reference to FIG. **5**.

In various situations, authentication of the key is needed **430** (e.g., by authentication module **310**). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application **330**). For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the biometric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user **440** as described below with reference to FIG. **6**. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

The code is utilized to authenticate the biometric key itself **450**, **460** as described below with reference to FIG. **7** and profile information is received. Responsive to successful authentication of the key, access is allowed **470** to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

FIG. **5** is a flow chart illustrating a method **500** for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks **510** an identification of the user and establishes a profile. The agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

The agent also collects and persistently stores **520** biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

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**).

FIG. **7** is a flow chart illustrating a method **700** for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received **710**. A request for authentication of the code is sent to the trusted key authority **720**. The trusted key authority determines whether the code is authentic **730** (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). 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 **740** (such as the user's age). If authentication is not successful, authentication fails **750** and the message to the application indicates that the user should be denied access.

In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. 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. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, 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. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of

computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

What is claimed is:

1. A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending 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, wherein the one or more codes and other data values includes the device ID code; and

responsive to authentication of the one or more codes and the other data values by the agent, receiving an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

2. The method of claim **1**, wherein the one or more codes and the other data values are transmitted to the agent over a network.

3. The method of claim **1**, further comprising:

registering an age verification for the user in association with the device ID code.

4. The method of claim **1**, wherein the one or more codes and the other data values indicate that the biometric verification was successful.

5. The method of claim **1**, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

6. The method of claim **1**, further comprising:

establishing a secure communication channel prior to sending the one or more codes and the other data values for authentication.

7. The method of claim **1**, further comprising:

receiving a request for the one or more codes and the other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and the other data values without a request for biometric verification, sending the one or more codes and the other data values without requesting the scan data.

8. An integrated device for verifying a user during authentication of the integrated device, comprising:

a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

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 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, wherein the one or more codes and the other data values includes the device ID code; and

responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

9. The integrated device of claim **8**, wherein the one or more codes and the other data values are transmitted to the agent over a network.

10. The integrated device of claim **9**, wherein an age verification is registered in association with the device ID code.

11. The integrated device of claim **8**, wherein the verifier comprises: an LED to be activated for requesting the biometric scan.

12. A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and the other data values comprises the device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and the other data values by the agent, wherein the authentication determines whether the one or more codes and the other data values are-legitimate;

receiving an access message from the agent; and

in response to a positive access message, allowing the biometrically verified user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

13. The method of claim **12**, further comprising:

registering a date of birth or age with the agent.

14. The method of claim **12**, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and the other data values associated with the biometrically verified user is received from the biometric key.

15. A system, comprising:

a biometric key stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending, one or more codes from the plurality of codes and other data values wherein the one or more codes and the other data values include the device ID code, and the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition; and

an authentication unit receives the plurality of codes and the other data values and send the plurality of codes and the other data values to agent for authentication to determine whether the one or more codes and the other data values are legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication unit receiving an access message from the agent allowing the user to access an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

16. The system of claim **15**, wherein the biometric key receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate the scan data.

17. The system of claim **15**, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and the other data values.

* * * * *

EXHIBIT 3

US008886954B1

(12) **United States Patent**
Giobbi

(10) **Patent No.: US 8,886,954 B1**
(45) **Date of Patent: *Nov. 11, 2014**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(71) Applicant: **Proxense, LLC**, Bend, OR (US)

(72) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/710,109**

(22) Filed: **Dec. 10, 2012**

Related U.S. Application Data

(63) Continuation of application No. 11/314,199, filed on Dec. 20, 2005, now Pat. No. 8,352,730.

(60) Provisional application No. 60/652,765, filed on Feb. 14, 2005, provisional application No. 60/637,538, filed on Dec. 20, 2004.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G05B 1/00 (2006.01)

(52) **U.S. Cl.**
CPC ***G05B 1/00*** (2013.01)
USPC **713/186**; 713/153

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,759,060 A 7/1988 Hayashi et al.
4,993,068 A 2/1991 Piosenka et al.
5,187,352 A 2/1993 Blair et al.
5,296,641 A 3/1994 Stelzel
5,392,433 A 2/1995 Hammersley et al.
5,416,780 A 5/1995 Patel

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO 00/62505 10/2000
WO WO 01/22724 3/2001

(Continued)

OTHER PUBLICATIONS

"Alliance Activities: Publications: Identity—Smart Card Alliance," Smart Card Alliance, 1997-2007, Retrieved on Jan. 7, 2007 from <URL:http://www.smartcardalliance.org/pages/publications-identity>, 3 pgs.

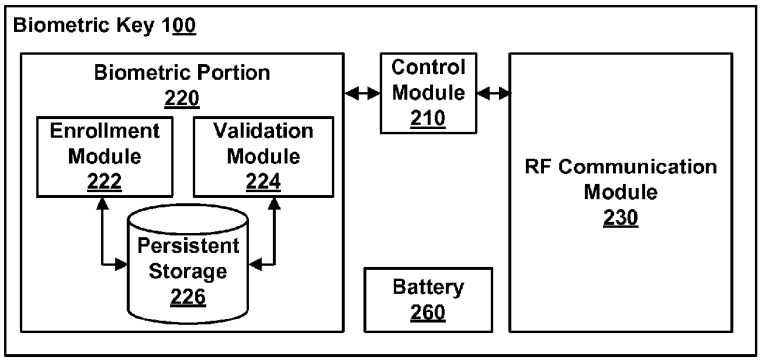
(Continued)

Primary Examiner — Eleni Shiferaw
Assistant Examiner — Phy Ahn Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

29 Claims, 6 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,422,632	A	6/1995	Bucholtz et al.	
5,450,489	A	9/1995	Ostrover et al.	
5,619,251	A	4/1997	Kuroiwa et al.	
5,629,980	A	5/1997	Stefik et al.	
5,644,354	A	7/1997	Thompson et al.	
5,666,412	A	9/1997	Handelman et al.	
5,784,464	A	7/1998	Akiyama et al.	
5,825,876	A	10/1998	Peterson, Jr.	
5,857,020	A	1/1999	Peterson, Jr.	
5,892,825	A	4/1999	Mages et al.	
5,894,551	A	4/1999	Huggins et al.	
5,898,880	A	4/1999	Ryu	
5,917,913	A	6/1999	Wang	
5,928,327	A	7/1999	Wang et al.	
5,991,399	A	11/1999	Graunke et al.	
5,991,749	A	11/1999	Morrill, Jr.	
6,016,476	A	1/2000	Maes et al.	
6,018,739	A	1/2000	McCoy et al.	
6,035,038	A	3/2000	Campinos et al.	
6,035,329	A	3/2000	Mages et al.	
6,038,334	A	3/2000	Hamid	
6,041,410	A *	3/2000	Hsu et al.	713/186
6,042,006	A	3/2000	Van Tilburg et al.	
6,055,314	A	4/2000	Spies et al.	
6,070,796	A	6/2000	Sirbu	
6,088,730	A	7/2000	Kato et al.	
6,104,334	A	8/2000	Allport	
6,121,544	A	9/2000	Petsinger	
6,148,142	A	11/2000	Anderson	
6,161,179	A	12/2000	Seidel	
6,185,316	B1	2/2001	Buffam	
6,209,089	B1	3/2001	Selitrennikoff et al.	
6,219,109	B1	4/2001	Raynesford et al.	
6,219,439	B1	4/2001	Burger	
6,247,130	B1	6/2001	Fritsch	
6,256,737	B1	7/2001	Bianco et al.	
6,266,415	B1	7/2001	Campinos et al.	
6,295,057	B1	9/2001	Rosin et al.	
6,336,121	B1	1/2002	Lyson et al.	
6,336,142	B1	1/2002	Kato et al.	
6,363,485	B1	3/2002	Adams et al.	
6,367,019	B1	4/2002	Ansell et al.	
6,381,747	B1	4/2002	Wonfor et al.	
6,385,596	B1	5/2002	Wiser et al.	
6,392,664	B1	5/2002	White et al.	
6,397,387	B1	5/2002	Rosin et al.	
6,401,059	B1	6/2002	Shen et al.	
6,411,307	B1	6/2002	Rosin et al.	
6,424,715	B1	7/2002	Saito	
6,425,084	B1	7/2002	Rallis et al.	
6,434,535	B1	8/2002	Kupka et al.	
6,446,130	B1	9/2002	Grapes	
6,463,534	B1	10/2002	Geiger et al.	
6,480,188	B1	11/2002	Horsley	
6,490,443	B1	12/2002	Freeny, Jr.	
6,510,350	B1	1/2003	Steen, III et al.	
6,523,113	B1	2/2003	Wehrenberg	
6,529,949	B1	3/2003	Getsin et al.	
6,546,418	B2	4/2003	Schena et al.	
6,550,011	B1	4/2003	Sims, III	
6,563,805	B1	5/2003	Ma et al.	
6,564,380	B1	5/2003	Murphy	
6,628,302	B2	9/2003	White et al.	
6,632,992	B2	10/2003	Hasegawa	
6,647,417	B1	11/2003	Hunter et al.	
6,667,684	B1	12/2003	Waggamon et al.	
6,683,954	B1	1/2004	Searle	
6,697,944	B1	2/2004	Jones et al.	
6,709,333	B1	3/2004	Bradford et al.	
6,711,464	B1	3/2004	Yap et al.	
6,775,655	B1	8/2004	Peinado et al.	
6,804,825	B1	10/2004	White et al.	
6,806,887	B2	10/2004	Chernock et al.	
6,850,147	B2	2/2005	Prokoski et al.	
6,873,975	B1	3/2005	Hatakeyama et al.	
6,950,941	B1	9/2005	Lee et al.	
6,963,971	B1 *	11/2005	Bush et al.	713/153
6,973,576	B2	12/2005	Giobbi	
6,975,202	B1	12/2005	Rodriguez et al.	
6,983,882	B2	1/2006	Cassone	
7,012,503	B2	3/2006	Nielsen	
7,090,126	B2	8/2006	Kelly et al.	
7,112,138	B2	9/2006	Hedrick et al.	
7,137,012	B1	11/2006	Kamibayashi et al.	
7,191,466	B1	3/2007	Hamid et al.	
7,218,944	B2	5/2007	Cromer et al.	
7,249,177	B1	7/2007	Miller	
7,305,560	B2	12/2007	Giobbi	
7,529,944	B2	5/2009	Hamid	
7,574,734	B2	8/2009	Fedronic et al.	
7,587,611	B2	9/2009	Johnson et al.	
7,617,523	B2 *	11/2009	Das et al.	726/5
7,644,443	B2	1/2010	Matsuyama et al.	
7,715,593	B1	5/2010	Adams et al.	
7,883,417	B2	2/2011	Bruzzese et al.	
7,904,718	B2	3/2011	Giobbi et al.	
2001/0044337	A1	11/2001	Rowe et al.	
2002/0007456	A1	1/2002	Peinado et al.	
2002/0013772	A1	1/2002	Peinado	
2002/0014954	A1	2/2002	Fitzgibbon et al.	
2002/0015494	A1	2/2002	Nagai et al.	
2002/0023032	A1	2/2002	Pearson et al.	
2002/0026424	A1	2/2002	Akashi	
2002/0071559	A1	6/2002	Christensen et al.	
2002/0073042	A1	6/2002	Maritzen et al.	
2002/0098888	A1	7/2002	Rowe et al.	
2002/0103027	A1	8/2002	Rowe et al.	
2002/0104006	A1	8/2002	Boate et al.	
2002/0108049	A1	8/2002	Xu et al.	
2002/0109580	A1	8/2002	Shreve et al.	
2002/0129262	A1 *	9/2002	Kutaragi et al.	713/193
2002/0138767	A1	9/2002	Hamid et al.	
2002/0140542	A1	10/2002	Prokoski et al.	
2002/0144117	A1	10/2002	Faigle	
2002/0150282	A1	10/2002	Kinsella	
2002/0152391	A1	10/2002	Willins et al.	
2002/0158750	A1	10/2002	Almalik	
2002/0174348	A1 *	11/2002	Ting	713/186
2002/0178063	A1	11/2002	Gravelle et al.	
2002/0191816	A1	12/2002	Maritzen et al.	
2003/0036425	A1	2/2003	Kaminkow et al.	
2003/0046552	A1	3/2003	Hamid	
2003/0054868	A1	3/2003	Paulsen et al.	
2003/0054881	A1	3/2003	Hedrick et al.	
2003/0055689	A1	3/2003	Block et al.	
2003/0079133	A1	4/2003	Breiter et al.	
2003/0115474	A1 *	6/2003	Khan et al.	713/186
2003/0127511	A1	7/2003	Kelly et al.	
2003/0139190	A1	7/2003	Steelberg et al.	
2003/0149744	A1 *	8/2003	Bierre et al.	709/217
2003/0172037	A1	9/2003	Jung et al.	
2003/0176218	A1	9/2003	LeMay et al.	
2003/0186739	A1	10/2003	Paulsen et al.	
2004/0127277	A1	7/2004	Walker et al.	
2004/0128162	A1 *	7/2004	Schlotterbeck et al.	705/2
2004/0129787	A1 *	7/2004	Saito et al.	235/492
2004/0209690	A1	10/2004	Bruzzese et al.	
2004/0209692	A1	10/2004	Schober et al.	
2004/0215615	A1	10/2004	Larsson et al.	
2004/0230488	A1	11/2004	Beenau et al.	
2005/0074126	A1 *	4/2005	Stanko	380/279
2005/0081040	A1	4/2005	Johnson et al.	
2005/0109836	A1 *	5/2005	Ben-Aissa	235/380
2005/0229007	A1	10/2005	Bolle et al.	
2005/0251688	A1	11/2005	Nanavati et al.	
2005/0253683	A1	11/2005	Lowe	
2006/0022046	A1	2/2006	Iwamura	
2006/0113381	A1	6/2006	Hochstein et al.	
2006/0156027	A1	7/2006	Blake	
2007/0220272	A1	9/2007	Campisi et al.	
2008/0019578	A1	1/2008	Saito et al.	
2008/0188308	A1	8/2008	Shepherd et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0328182	A1	12/2009	Malakapalli et al.
2010/0117794	A1	5/2010	Adams et al.
2011/0126188	A1	5/2011	Bernstein et al.

FOREIGN PATENT DOCUMENTS

WO	WO 01/75876	10/2001
WO	WO 01/77790	10/2001
WO	WO 2005/050450	6/2005
WO	WO 2005/086802	9/2005

OTHER PUBLICATIONS

"Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002, Retrieved on Jan. 7, 2007, from <URL:http://www.securitymagazine.com/CDA/Articles/technologies/3ae610eaa34d8010VgnVCM100000f932a8c0__>, 5 pgs.
Van Winkle, William, "Bluetooth, the King of Connectivity," Laptop Buyer's Guide and Handbook, Jan. 2000, pp. 148-153.
Yoshida, Junko, "Content Protection Plan Targets Wireless Home Networks," www.eetinnes.com, Jan. 11, 2002, 2 pgs.
Debow, Yvette, "Credit/Debit Debuts in Midwest Smart Card Test," Computers in Banking, v6, n11, Nov. 1989, 4 pgs.
Dennis, Sylvia, "Digital Passports Need Not Infringe Civil Liberties," Newsbytes, Dec. 2, 1999, 2 pgs.
Blum, Jonathan, "Digital Rights Management May Solver the Napster "Problem"," Technology Investor Industrysector, Oct. 2000, pp. 24-27.
Lake, Matt, "Downloading for Dollars," Sound & Vision, Nov. 2000, pp. 137-138.
Sapsford, Jathon, "E-Business: Sound Waves Could Help Ease Web-Fraud Woes," Wall Street Journal, Aug. 14, 2000, 2 pgs.
"Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet," Computergram International, Jan. 18, 1996, 2 pgs.
"Frequently Asked Questions (FAQs) About BioPay," BioPay, LLC, 2007, Retrieved on Jan. 7, 2007, from <URL: http://www.biopay.com/faqs-lowes.asp>, 5 pgs.
McIver, R. et al., "Identification and Verification Working Together," Bioscrypt, Aug. 27, 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20%20Verification%20Working%20-Together.pdf>, 5 pgs.
Weber, Thomas E., "In the Age of Napster, Protecting Copyright is a Digital Arms Race," Wall Street Journal, Jul. 24, 2000, 3 pgs.
PCT International Search Report, PCT/US04/38124, Apr. 7, 2005, 10 pgs.
PCT International Search Report, PCT/US05/43447, Feb. 22, 2007, 7 pgs.
PCT International Search Report, PCT/US05/46843, Mar. 1, 2007, 10 pgs.
PCT International Search Report, PCT/US07/11102, Oct. 3, 2008, 11 pgs.
PCT International Search Report, PCT/US07/11103, Apr. 23, 2008, 9 pgs.
PCT International Search Report, PCT/US07/11104, Jun. 26, 2008, 9 pgs.
PCT International Search Report, PCT/US07/11105, Oct. 20, 2008, 10 pgs.
Nilsson, J. et al., "Match-On-Card for Java Cards," Precise Biometrics, White Paper, Apr. 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf>, 5 pgs.
Nordin, B., "Match-On-Card Technology," Precise Biometrics, White Paper, Apr. 2004, Retrieved on Jan. 7, 2007, from <URL:http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precis%20Match-on-Card%20technology.pdf>, 7 pgs.
"Micronas and Thomson Multimedia Showcase a New Copy Protection System that Will Drive the Future of Digital Television," www.micronas.com, Jan. 8, 2002, 3 pgs.
Pope, "Oasis Digital Signature Services: Digital Signing without the Headaches," Internet Computing—IEEE, vol. 10, Oct. 2006, pp. 81-84.
"SAFModuleTM: A Look Into Strong Authentication," saflink Corporation, Retrieved on Jan. 7, 2007, from <URL: http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf>, 8 pgs.
"Say Hello to Bluetooth," Bluetooth Web site, Jun. 2000, 4 pgs.
"Smart Cards and Biometrics White Paper," Smart Card Alliance, May 2002, Retrieved on Jan. 7, 2007, from <URL: http://www.securitymanagementcom.library/smartcard_faqtech0802.pdf>, 7 pgs.
Lewis, Peter H., "Sony and Visa in On-Line Entertainment Venture," New York Times, v145, Nov. 16, 1995, 1 pg.
Fasca, Chad, "The Circuit," Electronic News, vol. 45 Iss. 45, Nov. 8, 1999, 2 pgs.
Wallace, Bob, "The Internet Unplugged," InformationWeek.com, Dec. 13, 1999, pp. 22-24.
Paget, Paul, "The Security Behind Secure Extranets," Enterprise Systems Journal, Dec. 1999, 4 pgs.
Kontzer, Tony, "Thomson Bets on Smart Cards for Video Encryption," www.informationweek.com, Jun. 7, 2001, p. 1.
Press Release, "Thomson Multimedia Unveils Copy Protection Proposal Designed to Provide Additional Layer of Digital Content Security," www.thompson-multimedia.com, May 30, 2001, 2 pgs.
Wade, Will, "Using Fingerprints to Make Payments at POS Slowly Gaining Popularity," Credit Union Journal, International Biometric Group, Apr. 21, 2003, Retrieved on Jan. 7, 2007, from <URL:http://www.biometricgroup.com/in_the_news/04.21.03.html>, 3 pgs.
Antonoff, Michael, "Visiting Video Valley," Sound & Vision, Nov. 2001, pp. 116, 118-119.
"What is a File?," Apr. 30, 1998, URL: http://unixhelp.ed.ac.uk/editors/whatisafile.html, accessed Mar. 11, 2010 via http://waybackmachine.org/1998061500000* /http://unixhelp.ed.ac.uk/editors/whatisafile.html, 1 pg.
Farouk, "Authentication Mechanisms in Grid Computing Environment; Comparative Study", 2012, IEEE, p. 1-6.

* cited by examiner

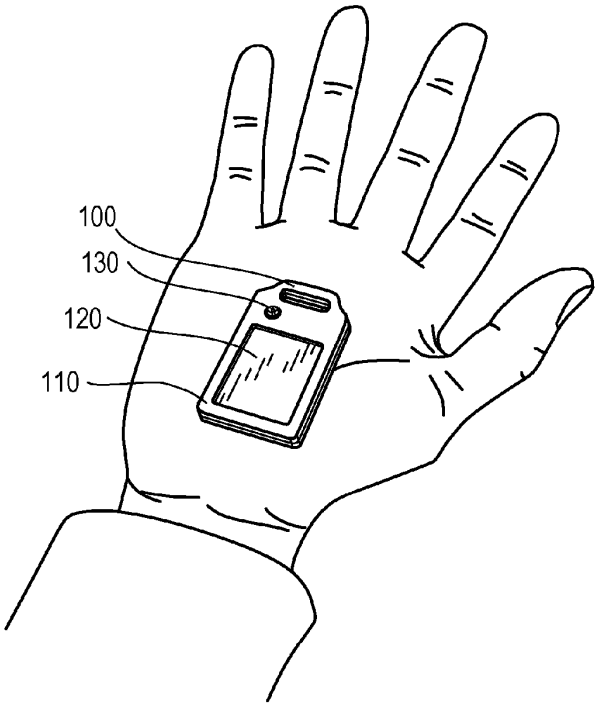

100
130
120
110

FIG. 1

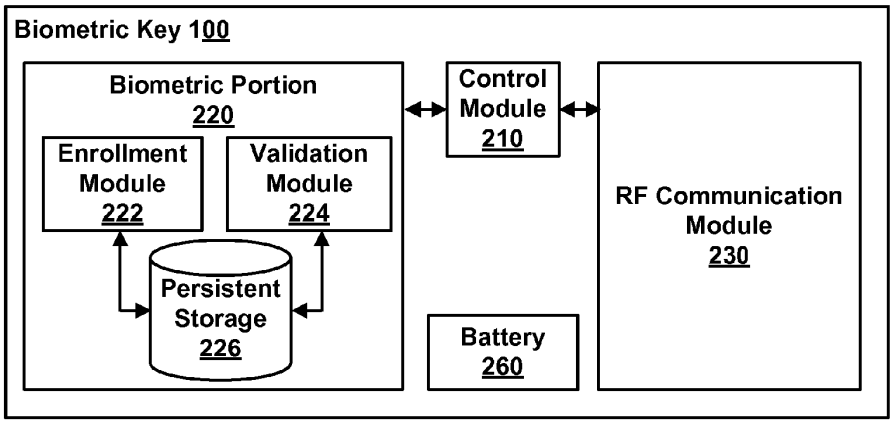

Biometric Key 100
Biometric Portion 220
Enrollment Module 222
Validation Module 224
Persistent Storage 226
Control Module 210
Battery 260
RF Communication Module 230

FIG. 2

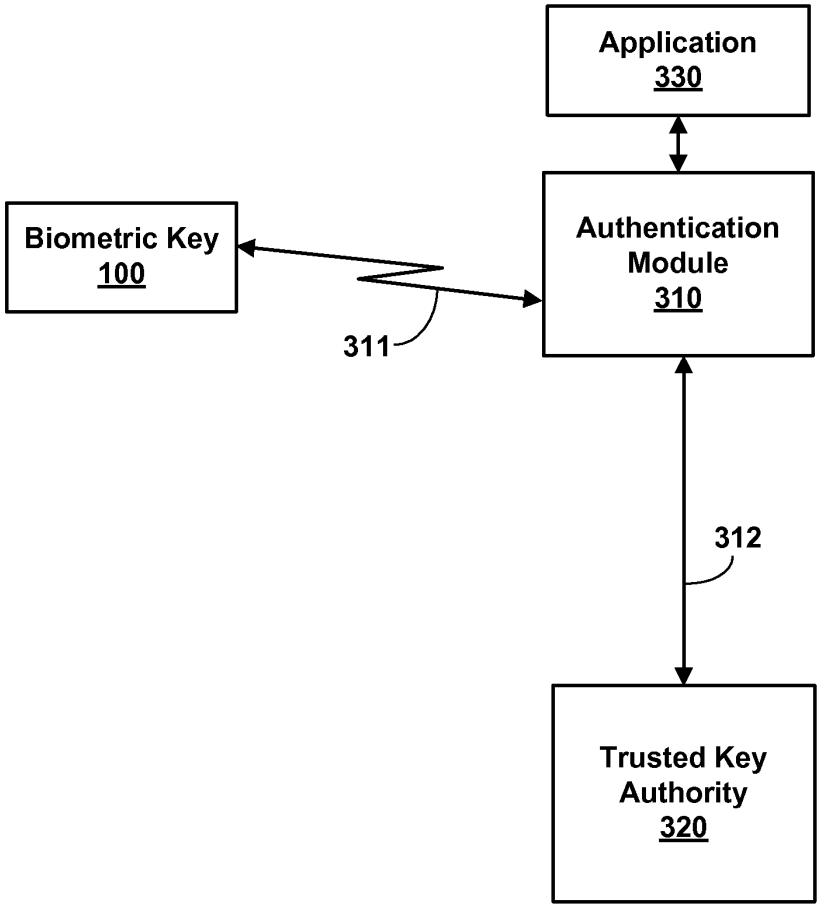

Application
330
Biometric Key
100
Authentication
Module
310
311
312
Trusted Key
Authority
320

FIG. 3

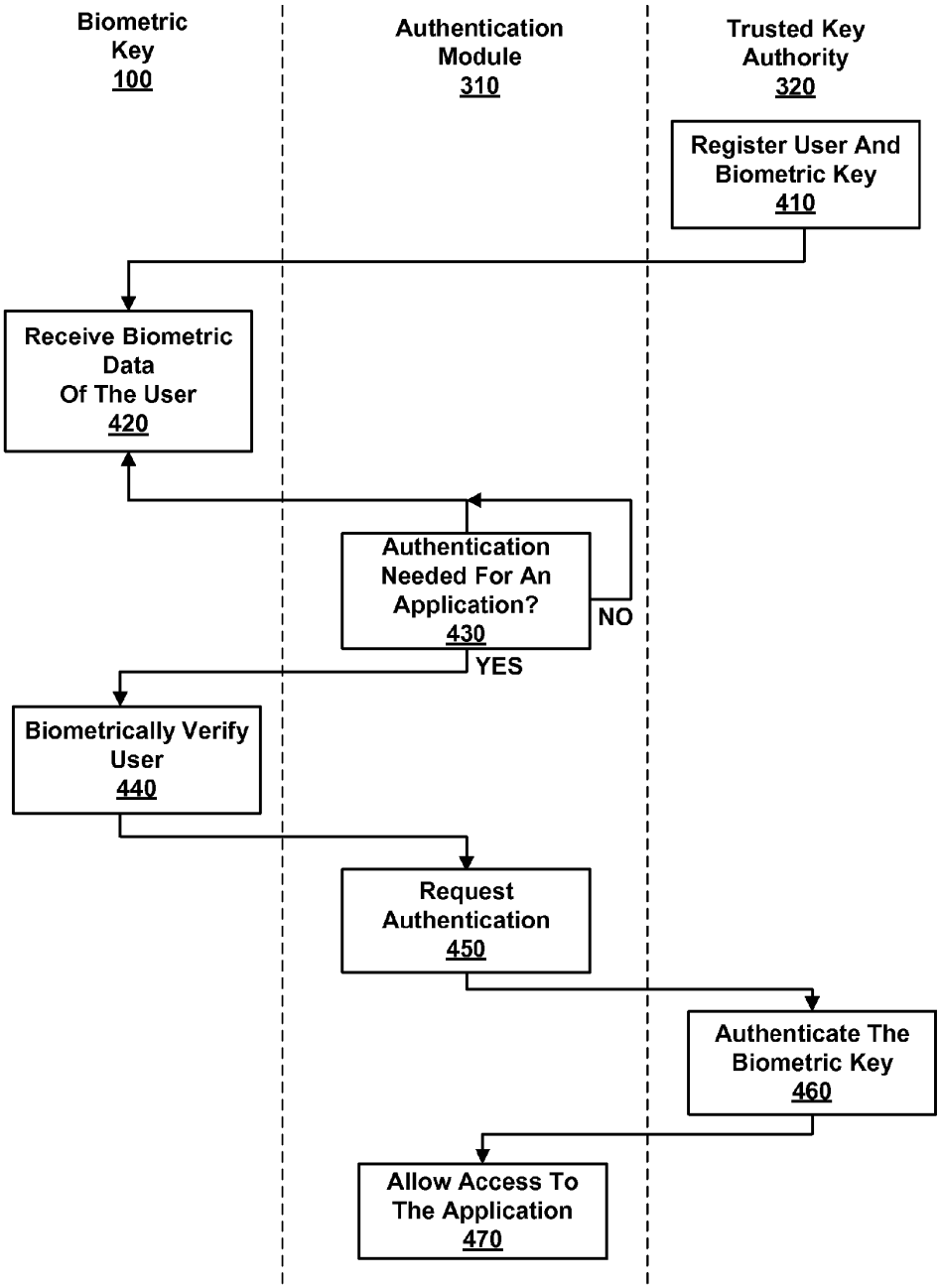

Biometric Key 100
Authentication Module 310
Trusted Key Authority 320
Register User And Biometric Key 410
Receive Biometric Data Of The User 420
Authentication Needed For An Application? 430
NO
YES
Biometrically Verify User 440
Request Authentication 450
Authenticate The Biometric Key 460
Allow Access To The Application 470

FIG. 4

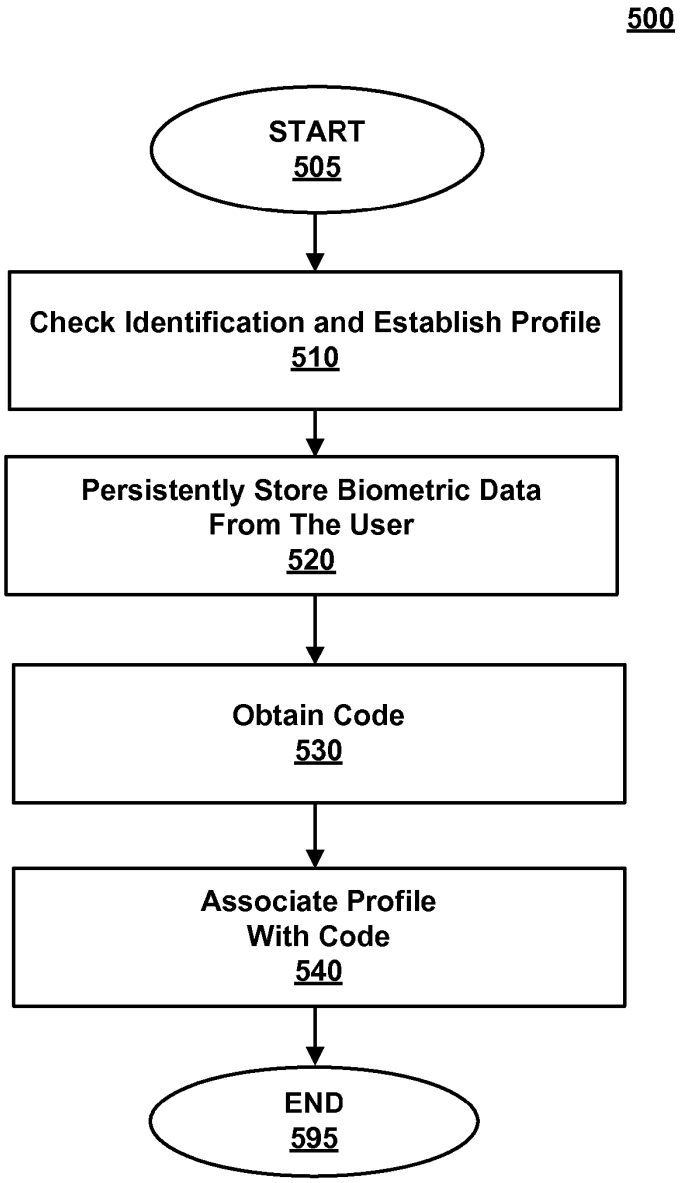

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data
From The User
520
Obtain Code
530
Associate Profile
With Code
540
END
595

FIG. 5

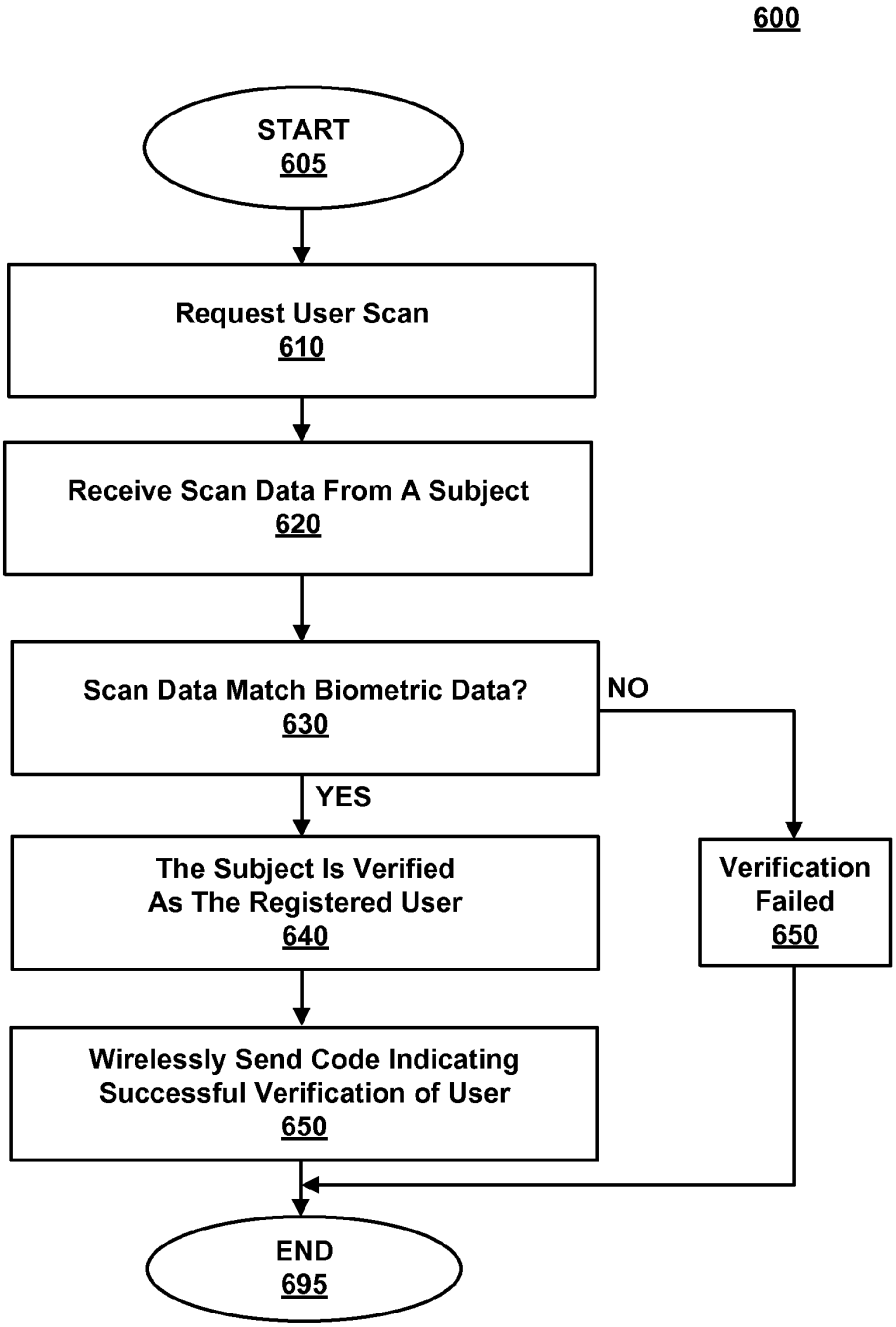

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

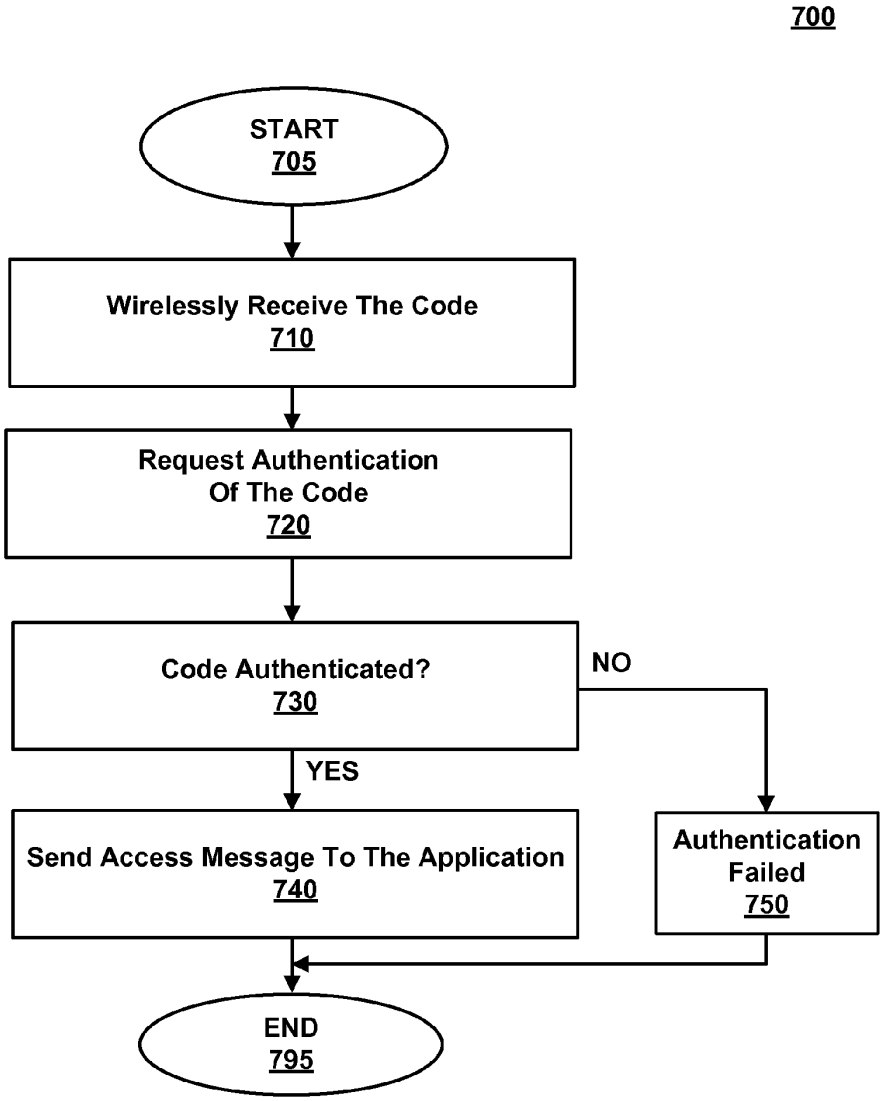

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority, under 35 U.S.C. §120, to U.S. patent application Ser. No. 11/314,199, filed Dec. 20, 2005 and entitled "Biometric Personal Data Key (PDK) Authentication," which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on Dec. 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on Feb. 14, 2005, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allowing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A uses often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, an integrated device includes a persistent storage to persistently stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format, and a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for

comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending a code for authentication.

In one embodiment, a method for verifying a user during authentication of an integrated device, includes persistently storing biometric data for the user in a tamper-resistant format; responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data to the biometric data to determine whether the data match; and responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance the operations further include registering an age verification for the user in association with the code. For instance the operations further include establishing a secure communication channel prior to sending the code for authentication. For instance the operations further include receiving a request for the code without a request for biometric verification, and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data. For instance, the features include: the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority; the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful; persistently storing biometric data includes permanently storing biometric data; the biometric data and the scan data are both based on a fingerprint scan by the user, an LED to be activated for requesting the biometric scan.

In one embodiment, a method for authenticating a verified user, includes receiving a code associated with a biometrically verified user; requesting authentication of the code; receiving an authentication result; and in response to the authentication result being positive, providing access to an application.

In one embodiment, a system includes an integrated device (e.g. a biometric key) to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code; and an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance, the operations further include registering the code with a trusted authority, wherein requesting authentication of the code includes providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority. For instance the operations further include registering a date of birth or age with the trusted authority. For instance the operations further include establishing a secure communications channel with an integrated device, wherein the code associated with the biometrically verified user is received from the integrated device. For instance the features include: the integrated device receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data; when the

integrated device cannot verify the scan data as being from the user, it does not send the code.

Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the integrated device can be authenticated for an application that is open to the public (i.e., in an open loop system).

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

FIG. **1** is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

FIG. **2** is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

FIG. **3** is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

FIG. **4** is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

FIG. **5** is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

FIG. **6** is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

FIG. **7** is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a fingerprint of a subject can be compared against previously-recorded biometric data for verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

FIG. **1** is a schematic diagram illustrating an example of a biometric key **100** for providing authentication information for a biometrically verified user according to one embodiment of the present invention. In one embodiment, the biometric key **100** comprises a frame **110**, a scan pad **120**, and an LED **130**. In one embodiment, biometric key **100** has a small form factor (e.g., the size of an automobile remote control) such that it can be unobtrusively carried by a user. In one embodiment, the biometric key **100** is integrated into another object or device. A device having an integrated biometric key **100** is occasionally referred to herein as an "integrated device." For example, in one embodiment, the biometric key **100** is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key **100** unobtrusive to carry.

Frame **110** can be formed by plastic, metal or another suitable material. Frame **110** is shaped to secure scan pad **120**, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame **110** is formed from a unitary molding to protect biometric data. Accordingly, frame **110** cannot be opened to expose the underlying components unless it is broken.

Scan pad **120** can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad **120** can be sized to fit a thumb or other finger. Biometric key **100** of the present embodiment includes LED **130** that lights up to request a fingerprint scan from a user. In one embodiment, LED **130** can also confirm that user verification and/or authentication has completed.

Biometric key **100** can authenticate a user for various purposes. For example, biometric key **100** can allow keyless entry into homes and autos. In another example, biometric key **100** can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key **100** can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key **100** operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

FIG. **2** is a block diagram illustrating biometric key **100** according to one embodiment of the present invention. Biometric key **100** comprises control module **210**, biometric portion **220**, RF communication module **230**, persistent storage **240**, and battery **250**. Biometric key **100** can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key **100** comprises a modified key fob.

Control module **210** coordinates between several functions of biometric key **100**. In one embodiment, control module **210** provides a verification code upon successful verification of the user. More specifically, once biometric portion **220** indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module **210** can trigger RF communication module **230** for sending a code indicating that the user was verified. In another embodiment, control module **210** can work in the opposite direction by detecting a request for verification from RF communication module **230**, and then requesting verification of the user from biometric portion **210**. Note that control module **210** of FIG. **2** is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key **100**.

Biometric portion **220** comprises enrollment module **222**, validation module **224**, and biometric data base **226**. In one embodiment, enrollment module **222** registers a user with biometric key **100** by persistently storing biometric data asso-

ciated with the user. Further, enrollment module **222** registers biometric key **100** with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key **100** to be stored therein.

Validation module **224** can comprise scan pad **120** (FIG. **1**) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module **214** determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module **224** can send comparison results to control module **210**.

In other embodiments, validation module **224** can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.

Persistent storage **226** persistently stores biometric data from one or more users which can be provided according to specific implementations. 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** can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. Persistent storage **226** is itself, and stores data in, a tamper-proof format to prevent any changes to the stored data. Tamperproofing 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.

In one embodiment, persistent storage **226** also stores the code that is provided by the key **100** responsive to successful verification of the user. As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key **100**. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments persistent storage **226** stores other data utilized during the operation of biometric key **100**. For example, persistent storage **226** can store encryption/decryption keys utilized to establish secure communications links.

Radio frequency (RF) communication module **230** is, for example, a transceiver or other mechanism for wireless communication. RF communication module **230** can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication **220** can be optimized for low-power usage by, for example, using short-range transceivers. RF communication module **230** can actively send out connection requests, or passively detect connection requests.

Battery **260** can be a conventional power source suitable for the components of biometric key **100**. Battery **260** can be either replaceable or rechargeable. Alternatively, battery **260** can be embedded within key **100** such that the key must be discarded or recycled upon expiration of the battery.

FIG. **3** is a block diagram illustrating a system **300** for providing authentication information for a biometrically verified user. System **300** comprises an authentication module **310** in communication with biometric key **100**, a trusted key authority **320**, and an application **330**.

Authentication module **310** is coupled in communication with biometric key via line **311** (i.e., a wireless medium such as EM signals), and with trusted key authority **320** via line **312** (e.g., a secure data network such as the Internet, or a cell network). Authentication module **310** can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module **310** servers as a gatekeeper to application **330** by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module **310** provides the code to trusted key authority **320** in order to verify that it belongs to a legitimate key (e.g., when application **330** is security-critical). 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**.

Application **330** is a resource that can be accessed by a verified and authenticated user. Application **330** can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information. Application **330** can execute on the same system as authentication module **310** or on another system in communication with the system of the authentication module. In one embodiment, application module **330** allows access by a user after receiving a message from authentication module **310**. At that point, application **330** can allow direct use by the user, or require that communications continue to pass through authentication module **310** for continued authentication.

Trusted key authority **320** is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, trusted key authority **320** verifies that a code from a biometric key is legitimate. To do so, the trusted key authority **320** stores a list of codes for legitimate biometric keys. The list can be batched or updated each time a new user/key is enrolled. In one embodiment, trusted key authority **320** can also store a profile associated with a biometric key. The profile describes the user associated with the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority **320** is provided by a server or other computerized device.

In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority **320** provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority **320** can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

FIG. **4** is a flow chart illustrating a method **400** for authenticating a biometrically verified user using a trusted key authority (e.g., authority **320**). A biometric key (e.g., biometric key **100**) is registered **410** with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled **420** with the biometric key as described below with reference to FIG. **5**.

In various situations, authentication of the key is needed **430** (e.g., by authentication module **310**). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application **330**). For example, a user can be standing proximate to a slot machine in a casino which

requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the biometric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user **440** as described below with reference to FIG. **6**. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

The code is utilized to authenticate the biometric key itself **450**, **460** as described below with reference to FIG. **7** and profile information is received. Responsive to successful authentication of the key, access is allowed 470 to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

FIG. **5** is a flow chart illustrating a method **500** for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks **510** an identification of the user and establishes a profile. The agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

The agent also collects and persistently stores **520** biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

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**).

FIG. **7** is a flow chart illustrating a method **700** for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received **710**. A request for authentication of the code is sent to the trusted key authority **720**. The trusted key authority determines whether the code is authentic **730** (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). 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 **740** (such as the user's age). If authentication is not successful, authentication fails **750** and the message to the application indicates that the user should be denied access.

In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. 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. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art.

An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, 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. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

What is claimed is:

1. A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is not capable of being subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

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.

2. The method of claim **1**, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

3. The method of claim **1**, further comprising:

registering an age verification for the user in association with the device ID code.

4. The method of claim **1**, wherein the one or more codes and other data values indicate that the biometric verification was successful.

5. The method of claim **1**, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

6. The method of claim **1**, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. The method of claim **1**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. The method of claim **1**, wherein the application includes a file including medical information.

9. The method of claim **1**, wherein the application includes a financial account.

10. The method of claim **1**, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values for authentication.

11. The method of claim **1**, further comprising:

receiving a request for the one or more codes and other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values without a request for biometric verification, sending the one or more codes and other data values without requesting the scan data.

12. An integrated device comprising:

a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper

proof format written to the persistent storage media and not capable of being subsequently altered;

a validation module, coupled to communicate with the persistent storage media, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allowing the user access to an application.

13. The integrated device of claim **12**, wherein the one or more codes and other data values are transmitted to the trusted authority over a network.

14. The integrated device of claim **12**, wherein an age verification is registered in association with the device ID code.

15. The integrated device of claim **12** comprising:

an LED to be activated for requesting the biometric scan.

16. A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with a trusted authority for authentication, the trusted authority operated by a third party;

requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority;

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 to the third party; and

in response to receiving the access message, allowing the biometrically verified user access to the application.

17. The method of claim **16**, further comprising:

registering a date of birth or age with the trusted authority.

18. The method of claim **16**, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.

19. The method of claim **16**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. The method of claim **16**, wherein the application includes a file including medical information.

21. The method of claim **16**, wherein the application includes a financial account.

22. A system, comprising:

an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated hardware device and a secret decryption value in a tamper proof format written to a storage element in the integrated hardware device that is not capable of being subsequently altered, and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and

an authentication circuit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority for authentication, and that receives an access message from the trusted authority indicating that the trusted authority successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.

23. The system of claim **22**, wherein the integrated hardware device receives an authentication request from the authentication circuit, and in response, requests a biometric scan from the user to generate scan data.

24. The system of claim **22**, wherein when the integrated hardware device cannot verify scan data as being from the user, the integrated hardware device does not send the one or more codes and other data values.

25. The system of claim **22**, wherein the integrated hardware device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. The system of claim **22**, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

27. The system of claim **22**, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. The system of claim **22**, wherein the application includes a file including medical information.

29. The system of claim **22**, wherein the application includes a financial account.

* * * * *

EXHIBIT 4

US010698989B2

(12) **United States Patent**
Giobbi

(10) **Patent No.: US 10,698,989 B2**
(45) **Date of Patent: *Jun. 30, 2020**

(54) **BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION**

(71) Applicant: **Proxense, LLC**, Bend, OR (US)

(72) Inventor: **John J. Giobbi**, Bend, OR (US)

(73) Assignee: **Proxense, LLC**, Bend, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/049,060**

(22) Filed: **Feb. 20, 2016**

(65) **Prior Publication Data**

US 2016/0171200 A1 Jun. 16, 2016

Related U.S. Application Data

(63) Continuation of application No. 14/521,982, filed on Oct. 23, 2014, now Pat. No. 9,298,905, which is a

(Continued)

(51) **Int. Cl.**
G06F 21/00 (2013.01)
G06F 21/32 (2013.01)

(Continued)

(52) **U.S. Cl.**
CPC ***G06F 21/32*** (2013.01); ***G05B 1/00*** (2013.01); ***G06F 21/35*** (2013.01); ***G07C 9/257*** (2020.01); ***H04L 9/321*** (2013.01)

(58) **Field of Classification Search**
CPC combination set(s) only.
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

3,739,329 A 6/1973 Lester
3,761,883 A 9/1973 Alvarez et al.

(Continued)

FOREIGN PATENT DOCUMENTS

JP H10-49604 2/1998
WO 0062505 A1 10/2000

(Continued)

OTHER PUBLICATIONS

"Rajendran Jeyaprakash, Jin Lee, Subir Biswas, Jae Mook Kim, Secured Smart Card Using Palm Vein Biometric On-card-Process, Aug. 28-30, 2008, IEEE Xplore, INSPEC #10205191" (Year: 2008).*

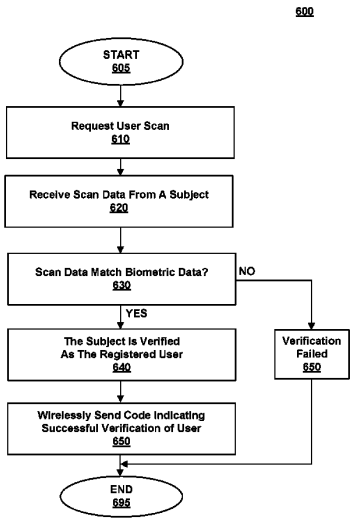
(Continued)

Primary Examiner — Phy Anh T Vu
(74) *Attorney, Agent, or Firm* — Patent Law Works LLP

(57) **ABSTRACT**

Systems and methods verifying a user during authentication of an integrated device. In one embodiment, the system includes an integrated device and an authentication unit. The integrated device stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format, and when scan data is verified by comparing the scan data to the biometric data, wirelessly sends one or more codes and other data values including the device ID code. The authentication unit receives and sends the one or more codes and the other data values to an agent for authentication, and receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

9 Claims, 6 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/710,109, filed on Dec. 10, 2012, now Pat. No. 8,886,954, which is a continuation of application No. 11/314,199, filed on Dec. 20, 2005, now Pat. No. 8,352,730.

(60) Provisional application No. 60/652,765, filed on Feb. 14, 2005, provisional application No. 60/637,538, filed on Dec. 20, 2004.

(51) **Int. Cl.**

G07C 9/25	(2020.01)
G06F 21/35	(2013.01)
G05B 1/00	(2006.01)
H04L 9/32	(2006.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,430,705 A 2/1984 Cannavino et al.
4,661,821 A 4/1987 Smith
4,759,060 A 7/1988 Hayashi et al.
4,993,068 A 2/1991 Piosenka et al.
5,187,352 A 2/1993 Blair et al.
5,224,164 A 6/1993 Elsner
5,296,641 A 3/1994 Stelzel
5,307,349 A 4/1994 Shloss et al.
5,317,572 A 5/1994 Satoh
5,325,285 A 6/1994 Araki
5,392,287 A 2/1995 Tiedemann, Jr. et al.
5,392,433 A 2/1995 Hammersley et al.
5,410,588 A 4/1995 Ito
5,416,780 A 5/1995 Patel
5,422,632 A 6/1995 Bucholtz et al.
5,428,684 A 6/1995 Akiyama et al.
5,450,489 A 9/1995 Ostrover et al.
5,473,690 A 12/1995 Grimonprez et al.
5,481,265 A 1/1996 Russell
5,506,863 A 4/1996 Meidan et al.
5,517,502 A 5/1996 Bestler et al.
5,541,583 A 7/1996 Mandelbaum
5,563,947 A 10/1996 Kikinis
5,589,838 A 12/1996 McEwan
5,594,227 A 1/1997 Deo
5,598,474 A * 1/1997 Johnson G06F 21/32 713/186
5,611,050 A 3/1997 Theimer et al.
5,619,251 A 4/1997 Kuroiwa et al.
5,623,552 A 4/1997 Lane
5,629,980 A 5/1997 Stefik et al.
5,644,354 A 7/1997 Thompson et al.
5,666,412 A 9/1997 Handelman et al.
5,689,529 A 11/1997 Johnson
5,692,049 A 11/1997 Johnson et al.
5,719,387 A 2/1998 Fujioka
5,729,237 A 3/1998 Webb
5,760,705 A 6/1998 Glessner et al.
5,760,744 A 6/1998 Sauer
5,773,954 A 6/1998 VanHorn
5,784,464 A 7/1998 Akiyama et al.
5,799,085 A 8/1998 Shona
5,825,876 A 10/1998 Peterson, Jr.
5,835,595 A 11/1998 Fraser et al.
5,838,306 A 11/1998 O'Connor et al.
5,854,891 A 12/1998 Postlewaite et al.
5,857,020 A 1/1999 Peterson, Jr.
5,886,634 A 3/1999 Muhme
5,892,825 A 4/1999 Mages et al.
5,892,900 A 4/1999 Ginter et al.
5,894,551 A 4/1999 Huggins et al.
5,898,880 A 4/1999 Ryu
5,910,776 A 6/1999 Black
5,917,913 A 6/1999 Wang
5,928,327 A 7/1999 Wang et al.
5,991,399 A 11/1999 Graunke et al.
5,991,749 A 11/1999 Morrill, Jr.
6,016,476 A 1/2000 Maes et al.
6,018,739 A 1/2000 McCoy
6,025,780 A 2/2000 Bowers
6,035,038 A 3/2000 Campinos et al.
6,035,329 A 3/2000 Mages et al.
6,038,334 A 3/2000 Hamid
6,040,786 A 3/2000 Fujioka
6,041,410 A * 3/2000 Hsu G06K 9/00013 380/285
6,042,006 A 3/2000 Van Tilburg et al.
6,055,314 A 4/2000 Spies et al.
6,070,796 A 6/2000 Sirbu
6,088,730 A 7/2000 Kato et al.
6,104,290 A 8/2000 Naguleswaran
6,104,334 A 8/2000 Allport
6,110,041 A 8/2000 Walker et al.
6,121,544 A 9/2000 Petsinger
6,134,283 A 10/2000 Sands et al.
6,138,010 A 10/2000 Rabe et al.
6,148,142 A 11/2000 Anderson
6,148,210 A 11/2000 Elwin et al.
6,161,179 A 12/2000 Seidel
6,177,887 B1 1/2001 Jerome
6,185,316 B1 2/2001 Buffam
6,209,089 B1 3/2001 Selitrennikoff et al.
6,219,109 B1 4/2001 Raynesford et al.
6,219,439 B1 4/2001 Burger
6,219,553 B1 4/2001 Panasik
6,237,848 B1 5/2001 Everett
6,240,076 B1 5/2001 Kanerva et al.
6,247,130 B1 6/2001 Fritsch
6,249,869 B1 6/2001 Drupsteen et al.
6,256,737 B1 7/2001 Bianco et al.
6,266,415 B1 7/2001 Campinos et al.
6,270,011 B1 * 8/2001 Gottfried G06F 21/32 235/379
6,279,111 B1 8/2001 Jensenworth et al.
6,279,146 B1 8/2001 Evans et al.
6,295,057 B1 9/2001 Rosin et al.
6,325,285 B1 12/2001 Baratelli
6,336,121 B1 1/2002 Lyson et al.
6,336,142 B1 1/2002 Kato et al.
6,343,280 B2 1/2002 Clark
6,345,347 B1 2/2002 Biran
6,363,485 B1 3/2002 Adams et al.
6,367,019 B1 4/2002 Ansell et al.
6,369,693 B1 4/2002 Gibson
6,370,376 B1 4/2002 Sheath
6,381,747 B1 4/2002 Wonfor et al.
6,385,596 B1 5/2002 Wiser et al.
6,392,664 B1 5/2002 White et al.
6,397,387 B1 5/2002 Rosin et al.
6,401,059 B1 6/2002 Shen et al.
6,411,307 B1 6/2002 Rosin et al.
6,424,249 B1 7/2002 Houvener
6,424,715 B1 7/2002 Saito
6,425,084 B1 7/2002 Rallis et al.
6,434,403 B1 8/2002 Ausems et al.
6,434,535 B1 8/2002 Kupka et al.
6,446,130 B1 9/2002 Grapes
6,463,534 B1 10/2002 Geiger et al.
6,480,101 B1 11/2002 Kelly et al.
6,480,188 B1 11/2002 Horsley
6,484,946 B2 11/2002 Matsumoto et al.
6,487,663 B1 11/2002 Jaisimha et al.
6,490,443 B1 12/2002 Freeny, Jr.
6,510,350 B1 1/2003 Steen, III et al.
6,522,253 B1 2/2003 Saltus
6,523,113 B1 2/2003 Wehrenberg
6,529,949 B1 3/2003 Getsin et al.
6,546,418 B2 4/2003 Schena et al.
6,550,011 B1 4/2003 Sims, III
6,563,465 B2 5/2003 Frecska
6,563,805 B1 5/2003 Ma et al.
6,564,380 B1 5/2003 Murphy
6,577,238 B1 6/2003 Whitesmith et al.
6,593,887 B2 7/2003 Luk et al.
6,597,680 B1 7/2003 Lindskog et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,607,136	B1	8/2003	Atsmon et al.
6,628,302	B2	9/2003	White et al.
6,632,992	B2	10/2003	Hasegawa
6,633,981	B1	10/2003	Davis
6,645,077	B2	11/2003	Rowe
6,647,417	B1	11/2003	Hunter et al.
6,657,538	B1	12/2003	Ritter
6,658,566	B1	12/2003	Hazard
6,667,684	B1	12/2003	Waggamon et al.
6,669,096	B1	12/2003	Saphar et al.
6,671,808	B1	12/2003	Abbott et al.
6,683,954	B1	1/2004	Searle
6,697,944	B1	2/2004	Jones et al.
6,709,333	B1	3/2004	Bradford et al.
6,711,464	B1	3/2004	Yap et al.
6,714,168	B2	3/2004	Berenbaum
6,715,246	B1	4/2004	Frecska et al.
6,728,397	B2	4/2004	McNeal
6,737,955	B2	5/2004	Ghabra et al.
6,758,394	B2	7/2004	Maskatiya et al.
6,771,969	B1	8/2004	Chinoy et al.
6,775,655	B1	8/2004	Peinado et al.
6,785,474	B2	8/2004	Hirt et al.
6,788,640	B2	9/2004	Celeste
6,788,924	B1	9/2004	Knutson et al.
6,795,425	B1	9/2004	Raith
6,804,825	B1	10/2004	White et al.
6,806,887	B2	10/2004	Chernock et al.
6,839,542	B2	1/2005	Sibecas et al.
6,850,147	B2	2/2005	Prokoski et al.
6,853,988	B1	2/2005	Dickinson et al.
6,859,812	B1	2/2005	Poynor
6,861,980	B1	3/2005	Rowitch et al.
6,873,975	B1	3/2005	Hatakeyama et al.
6,879,567	B2	4/2005	Callaway et al.
6,879,966	B1	4/2005	Lapsley et al.
6,886,741	B1	5/2005	Salveson
6,889,067	B2	5/2005	Willey
6,891,822	B1	5/2005	Gubbi et al.
6,892,307	B1	5/2005	Wood et al.
6,930,643	B2	8/2005	Byrne et al.
6,947,003	B2	9/2005	Fluor
6,950,941	B1	9/2005	Lee et al.
6,957,086	B2	10/2005	Bahl et al.
6,963,270	B1	11/2005	Gallagher, III et al.
6,963,971	B1	11/2005	Bush et al.
6,973,576	B2	12/2005	Giobbi
6,975,202	B1	12/2005	Rodriguez et al.
6,980,087	B2	12/2005	Zukowski
6,983,882	B2	1/2006	Cassone
6,999,032	B2	2/2006	Pakray et al.
7,012,503	B2	3/2006	Nielsen
7,031,945	B1	4/2006	Donner
7,049,963	B2	5/2006	Waterhouse et al.
7,055,171	B1	5/2006	Martin et al.
7,058,806	B2	6/2006	Smeets et al.
7,061,380	B1	6/2006	Orlando et al.
7,068,623	B1	6/2006	Barany et al.
7,072,900	B2	7/2006	Sweitzer et al.
7,079,079	B2	7/2006	Jo et al.
7,090,126	B2	8/2006	Kelly et al.
7,100,053	B1	8/2006	Brown et al.
7,111,789	B2	9/2006	Rajasekaran et al.
7,112,138	B2	9/2006	Hedrick et al.
7,119,659	B2	10/2006	Bonalle et al.
7,123,149	B2	10/2006	Nowak et al.
7,130,668	B2	10/2006	Chang et al.
7,137,008	B1	11/2006	Hamid
7,137,012	B1	11/2006	Kamibayashi et al.
7,139,914	B2	11/2006	Arnouse
7,155,416	B2	12/2006	Shatford
7,159,114	B1	1/2007	Zajkowski et al.
7,159,765	B2	1/2007	Frerking
7,167,987	B2	1/2007	Angelo
7,168,089	B2	1/2007	Nguyen et al.
7,167,797	B2	2/2007	Zai et al.
7,191,466	B1	3/2007	Hamid et al.
7,209,955	B1	4/2007	Major et al.
7,218,944	B2	5/2007	Cromer et al.
7,225,161	B2	5/2007	Lam et al.
7,230,908	B2	6/2007	Vanderaar et al.
7,231,068	B2	6/2007	Tibor
7,231,451	B2	6/2007	Law et al.
7,242,923	B2	7/2007	Perera et al.
7,249,177	B1	7/2007	Miller
7,272,723	B1	9/2007	Abbott et al.
7,277,737	B1	10/2007	Vollmer et al.
7,278,025	B2	10/2007	Saito
7,295,119	B2	11/2007	Rappaport et al.
7,305,560	B2	12/2007	Giobbi
7,310,042	B2	12/2007	Seifert
7,314,164	B2	1/2008	Bonalle
7,317,799	B2	1/2008	Hammersmith et al.
7,319,395	B2	1/2008	Puzio et al.
7,330,108	B2	2/2008	Thomas
7,333,002	B2	2/2008	Bixler et al.
7,336,181	B2	2/2008	Nowak et al.
7,336,182	B1	2/2008	Baranowski et al.
7,337,326	B2	2/2008	Palmer et al.
7,341,181	B2	3/2008	Bonalle
7,349,557	B2	3/2008	Tibor
7,356,393	B1	4/2008	Schlatre et al.
7,356,706	B2	4/2008	Scheurich
7,361,919	B2	4/2008	Setlak
7,370,366	B2	5/2008	Lacan et al.
7,380,202	B1	5/2008	Lindhorst et al.
7,382,799	B1	6/2008	Young et al.
7,387,235	B2	6/2008	Gilbert et al.
7,401,731	B1	7/2008	Pletz et al.
7,424,134	B2	9/2008	Chou
7,447,911	B2	11/2008	Chou et al.
7,458,510	B1	12/2008	Zhou
7,460,836	B2	12/2008	Smith et al.
7,461,444	B2	12/2008	Deaett et al.
7,466,232	B2	12/2008	Neuwirth
7,472,280	B2	12/2008	Giobbi
7,512,806	B2	3/2009	Lemke
7,525,413	B2	4/2009	Jung et al.
7,529,944	B2	5/2009	Hamid
7,545,312	B2	6/2009	Kiang et al.
7,565,329	B2	7/2009	Lapsley et al.
7,573,382	B2	8/2009	Choubey et al.
7,573,841	B2	8/2009	Lee et al.
7,574,734	B2	8/2009	Fedronic et al.
7,583,238	B2	9/2009	Cassen et al.
7,583,643	B2	9/2009	Smith et al.
7,587,611	B2	9/2009	Johnson et al.
7,595,765	B1	9/2009	Hirsch
7,603,564	B2	10/2009	Adachi
7,606,733	B2	10/2009	Shmueli et al.
7,617,523	B2	11/2009	Das et al.
7,620,184	B2	11/2009	Marque Pucheu
7,624,417	B2	11/2009	Dua
7,640,273	B2	12/2009	Wallmeier et al.
7,644,443	B2	1/2010	Matsuyama et al.
7,646,307	B2	1/2010	Plocher et al.
7,652,892	B2	1/2010	Shiu et al.
7,676,380	B2	3/2010	Graves et al.
7,711,152	B1	5/2010	Davida et al.
7,715,593	B1	5/2010	Adams et al.
7,724,717	B2	5/2010	Porras et al.
7,724,720	B2	5/2010	Korpela et al.
7,764,236	B2	7/2010	Hill et al.
7,765,181	B2	7/2010	Thomas et al.
7,773,754	B2	8/2010	Buer et al.
7,774,613	B2	8/2010	Lemke
7,780,082	B2	8/2010	Handa et al.
7,796,551	B1	9/2010	Machiraju et al.
7,813,822	B1	10/2010	Hoffberg
7,865,448	B2	1/2011	Pizarro
7,883,417	B2	2/2011	Bruzzese et al.
7,904,718	B2	3/2011	Giobbi et al.
7,943,868	B2	5/2011	Anders et al.
7,957,536	B2	6/2011	Nolte

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,961,078	B1	6/2011	Reynolds et al.	
7,984,064	B2	7/2011	Fusari	
7,996,514	B2	8/2011	Baumert et al.	
8,026,821	B2	9/2011	Reeder et al.	
8,036,152	B2	10/2011	Brown et al.	
8,077,041	B2	12/2011	Stern et al.	
8,081,215	B2	12/2011	Kuo et al.	
8,082,160	B2	12/2011	Collins, Jr. et al.	
8,089,354	B2	1/2012	Perkins	
8,112,066	B2	2/2012	Ben Ayed	
8,135,624	B1	3/2012	Ramalingam et al.	
8,171,528	B1	5/2012	Brown	
8,193,923	B2	6/2012	Rork et al.	
8,215,552	B1	7/2012	Rambadt	
8,248,263	B2	8/2012	Shervey et al.	
8,258,942	B1	9/2012	Lanzone et al.	
8,294,554	B2	10/2012	Shoarinejad et al.	
8,296,573	B2	10/2012	Bolle et al.	
8,307,414	B2	11/2012	Zerfos et al.	
8,325,011	B2	12/2012	Butler et al.	
8,340,672	B2	12/2012	Brown et al.	
8,352,730	B2	1/2013	Giobbi	
8,373,562	B1	2/2013	Heinze et al.	
8,387,124	B2	2/2013	Smetters et al.	
8,390,456	B2	3/2013	Puleston et al.	
8,395,484	B2	3/2013	Fullerton	
8,410,906	B1	4/2013	Dacus et al.	
8,421,606	B2	4/2013	Collins, Jr. et al.	
8,424,079	B2	4/2013	Adams et al.	
8,432,262	B2	4/2013	Talty et al.	
8,433,919	B2	4/2013	Giobbi et al.	
8,484,696	B2	7/2013	Gatto et al.	
8,494,576	B1	7/2013	Bye et al.	
8,508,336	B2	8/2013	Giobbi et al.	
8,519,823	B2	8/2013	Rinkes	
8,522,019	B2	8/2013	Michaelis	
8,558,699	B2	10/2013	Butler et al.	
8,577,091	B2	11/2013	Ivanov et al.	
8,646,042	B1	2/2014	Brown	
8,678,273	B2	3/2014	McNeal	
8,738,925	B1	5/2014	Park et al.	
8,799,574	B2	8/2014	Corda	
8,856,539	B2	10/2014	Weiss	
8,914,477	B2	12/2014	Gammon	
8,918,854	B1	12/2014	Giobbi	
8,931,698	B2	1/2015	Ishikawa et al.	
8,979,646	B2	3/2015	Moser et al.	
9,037,140	B1	5/2015	Brown	
9,049,188	B1	6/2015	Brown	
9,230,399	B2	1/2016	Yacenda	
9,235,700	B1	1/2016	Brown	
9,276,914	B2	3/2016	Woodward et al.	
9,305,312	B2	4/2016	Kountotsis et al.	
9,405,898	B2	8/2016	Giobbi	
9,418,205	B2	8/2016	Giobbi	
9,542,542	B2	1/2017	Giobbi et al.	
9,679,289	B1	6/2017	Brown	
9,892,250	B2	2/2018	Giobbi	
10,073,960	B1	9/2018	Brown	
10,110,385	B1	10/2018	Rush et al.	
2001/0024428	A1	9/2001	Onouchi	
2001/0026619	A1	10/2001	Howard	
2001/0027121	A1	10/2001	Boesen	
2001/0027439	A1	10/2001	Holtzman et al.	
2001/0044337	A1	11/2001	Rowe et al.	
2002/0004783	A1	1/2002	Paltenghe et al.	
2002/0007456	A1	1/2002	Peinado et al.	
2002/0010679	A1	1/2002	Felsher	
2002/0013772	A1	1/2002	Peinado	
2002/0014954	A1	2/2002	Fitzgibbon et al.	
2002/0015494	A1	2/2002	Nagai et al.	
2002/0019811	A1	2/2002	Lapsley et al.	
2002/0022455	A1	2/2002	Salokannel et al.	
2002/0023032	A1	2/2002	Pearson	
2002/0023217	A1*	2/2002	Wheeler	G06F 21/32 713/171
2002/0026424	A1	2/2002	Akashi	
2002/0037732	A1	3/2002	Gous et al.	
2002/0052193	A1	5/2002	Chetty	
2002/0055908	A1	5/2002	Di Giorgio et al.	
2002/0056043	A1	5/2002	Glass	
2002/0062249	A1	5/2002	Iannacci	
2002/0068605	A1	6/2002	Stanley	
2002/0071559	A1	6/2002	Christensen	
2002/0073042	A1	6/2002	Maritzen et al.	
2002/0080969	A1	6/2002	Giobbi	
2002/0083318	A1	6/2002	Larose	
2002/0086690	A1	7/2002	Takahashi et al.	
2002/0089890	A1	7/2002	Fibranz et al.	
2002/0091646	A1	7/2002	Lake	
2002/0095586	A1*	7/2002	Doyle	G06F 21/32 713/186
2002/0095587	A1*	7/2002	Doyle	G07F 7/1008 713/186
2002/0098888	A1	7/2002	Rowe et al.	
2002/0100798	A1	8/2002	Farrugia et al.	
2002/0103027	A1	8/2002	Rowe et al.	
2002/0104006	A1	8/2002	Boate	
2002/0104019	A1	8/2002	Chatani	
2002/0105918	A1	8/2002	Yamada et al.	
2002/0108049	A1	8/2002	Xu et al.	
2002/0109580	A1*	8/2002	Shreve	G07C 9/00103 340/5.61
2002/0111919	A1	8/2002	Weller et al.	
2002/0116615	A1	8/2002	Nguyen	
2002/0124251	A1	9/2002	Hunter et al.	
2002/0128017	A1	9/2002	Virtanen	
2002/0129262	A1*	9/2002	Kutaragi	G06F 21/10 713/193
2002/0138438	A1*	9/2002	Bardwell	G06F 21/32 705/51
2002/0138767	A1	9/2002	Hamid et al.	
2002/0140542	A1	10/2002	Prokoski et al.	
2002/0141586	A1	10/2002	Margalit et al.	
2002/0143623	A1	10/2002	Dayley	
2002/0143655	A1	10/2002	Elston et al.	
2002/0144117	A1	10/2002	Faigle	
2002/0147653	A1	10/2002	Shmueli et al.	
2002/0148892	A1*	10/2002	Bardwell	G06F 21/32 235/380
2002/0150282	A1	10/2002	Kinsella	
2002/0152391	A1	10/2002	Willins et al.	
2002/0153996	A1	10/2002	Chan et al.	
2002/0158121	A1*	10/2002	Stanford-Clark	G06Q 20/341 235/375
2002/0158750	A1	10/2002	Almalik	
2002/0158765	A1	10/2002	Pape et al.	
2002/0160820	A1	10/2002	Winkler	
2002/0174348	A1	11/2002	Ting	
2002/0177460	A1	11/2002	Beasley et al.	
2002/0178063	A1	11/2002	Gravelle et al.	
2002/0191816	A1	12/2002	Maritzen et al.	
2002/0196963	A1*	12/2002	Bardwell	G06F 21/32 382/124
2002/0199120	A1	12/2002	Schmidt	
2003/0022701	A1	1/2003	Gupta	
2003/0034877	A1	2/2003	Miller et al.	
2003/0036416	A1	2/2003	Pattabiraman et al.	
2003/0036425	A1	2/2003	Kaminkow et al.	
2003/0046228	A1	3/2003	Berney	
2003/0046552	A1	3/2003	Hamid	
2003/0051173	A1*	3/2003	Krueger	G06F 21/32 726/21
2003/0054868	A1	3/2003	Paulsen et al.	
2003/0054881	A1	3/2003	Hedrick et al.	
2003/0055689	A1	3/2003	Block et al.	
2003/0063619	A1	4/2003	Montano et al.	
2003/0079133	A1	4/2003	Breiter et al.	
2003/0088441	A1	5/2003	McNerney	
2003/0109274	A1	6/2003	Budka et al.	
2003/0115351	A1	6/2003	Giobbi	
2003/0115474	A1	6/2003	Khan	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0117969 A1 6/2003 Koo et al.
2003/0117980 A1 6/2003 Kim et al.
2003/0120934 A1* 6/2003 Ortiz H04L 63/0861 713/186
2003/0127511 A1 7/2003 Kelly et al.
2003/0128866 A1 7/2003 McNeal
2003/0137404 A1 7/2003 Bonneau, Jr. et al.
2003/0139190 A1 7/2003 Steelberg et al.
2003/0146835 A1 8/2003 Carter
2003/0149744 A1 8/2003 Bierre
2003/0163388 A1 8/2003 Beane
2003/0167207 A1 9/2003 Berardi et al.
2003/0169697 A1 9/2003 Suzuki et al.
2003/0172037 A1 9/2003 Jung
2003/0174839 A1 9/2003 Yamagata et al.
2003/0176218 A1 9/2003 LeMay et al.
2003/0186739 A1 10/2003 Paulsen et al.
2003/0195842 A1 10/2003 Reece
2003/0213840 A1 11/2003 Livingston et al.
2003/0223394 A1 12/2003 Parantainen et al.
2003/0225703 A1 12/2003 Angel
2003/0226031 A1 12/2003 Proudler et al.
2003/0233458 A1 12/2003 Kwon et al.
2004/0002347 A1 1/2004 Hoctor et al.
2004/0015403 A1 1/2004 Moskowitz et al.
2004/0022384 A1* 2/2004 Flores H04M 3/38 379/265.13
2004/0029620 A1 2/2004 Karaoguz
2004/0029635 A1 2/2004 Giobbi
2004/0030764 A1 2/2004 Birk et al.
2004/0030894 A1 2/2004 Labrou et al.
2004/0035644 A1 2/2004 Ford et al.
2004/0039909 A1 2/2004 Cheng
2004/0048570 A1 3/2004 Oba et al.
2004/0048609 A1 3/2004 Kosaka
2004/0059682 A1 3/2004 Hasumi et al.
2004/0059912 A1 3/2004 Zizzi
2004/0064728 A1 4/2004 Scheurich
2004/0068656 A1 4/2004 Lu
2004/0073792 A1 4/2004 Noble et al.
2004/0081127 A1 4/2004 Gardner et al.
2004/0082385 A1 4/2004 Silva et al.
2004/0098597 A1 5/2004 Giobbi
2004/0114563 A1 6/2004 Shvodian
2004/0117644 A1 6/2004 Colvin
2004/0123106 A1 6/2004 D'Angelo et al.
2004/0123127 A1 6/2004 Teicher
2004/0127277 A1 7/2004 Walker et al.
2004/0128162 A1 7/2004 Schlotterbeck et al.
2004/0128389 A1 7/2004 Kopchik
2004/0128500 A1 7/2004 Cihula et al.
2004/0128508 A1 7/2004 Wheeler et al.
2004/0129787 A1* 7/2004 Saito G06K 19/07 235/492
2004/0137912 A1 7/2004 Lin
2004/0158746 A1 8/2004 Hu et al.
2004/0166875 A1 8/2004 Jenkins et al.
2004/0167465 A1 8/2004 Mihai et al.
2004/0193925 A1 9/2004 Safriel
2004/0203923 A1 10/2004 Mullen
2004/0208139 A1 10/2004 Iwamura
2004/0209690 A1 10/2004 Bruzzese et al.
2004/0209692 A1 10/2004 Schober et al.
2004/0214582 A1 10/2004 Lan et al.
2004/0215615 A1 10/2004 Larsson et al.
2004/0217859 A1 11/2004 Pucci et al.
2004/0218581 A1 11/2004 Cattaneo
2004/0222877 A1 11/2004 Teramura et al.
2004/0230488 A1 11/2004 Beenau et al.
2004/0234117 A1 11/2004 Tibor
2004/0243519 A1 12/2004 Perttila et al.
2004/0246103 A1 12/2004 Zukowski
2004/0246950 A1 12/2004 Parker et al.
2004/0252659 A1 12/2004 Yun et al.
2004/0253996 A1 12/2004 Chen et al.
2004/0254837 A1 12/2004 Roshkoff
2004/0255139 A1 12/2004 Giobbi
2004/0255145 A1 12/2004 Chow
2005/0001028 A1 1/2005 Zuili
2005/0002028 A1 1/2005 Kasapi et al.
2005/0005136 A1* 1/2005 Chen H04L 9/3073 713/186
2005/0006452 A1 1/2005 Aupperle
2005/0025093 A1 2/2005 Yun et al.
2005/0028168 A1 2/2005 Marcjan
2005/0035897 A1 2/2005 Perl et al.
2005/0039027 A1* 2/2005 Shapiro G06F 21/32 713/186
2005/0040961 A1 2/2005 Tuttle
2005/0047386 A1 3/2005 Yi
2005/0049013 A1 3/2005 Chang et al.
2005/0050208 A1 3/2005 Chatani
2005/0050324 A1 3/2005 Corbett et al.
2005/0054431 A1 3/2005 Walker et al.
2005/0055242 A1 3/2005 Bello et al.
2005/0055244 A1 3/2005 Mullan et al.
2005/0058292 A1 3/2005 Diorio et al.
2005/0074126 A1* 4/2005 Stanko H04L 63/0807 380/279
2005/0076242 A1 4/2005 Breuer
2005/0081040 A1 4/2005 Johnson et al.
2005/0086115 A1 4/2005 Pearson
2005/0089000 A1 4/2005 Bae et al.
2005/0090200 A1 4/2005 Karaoguz et al.
2005/0091338 A1 4/2005 de la Huerga
2005/0094657 A1 5/2005 Sung et al.
2005/0097037 A1 5/2005 Tibor
2005/0105600 A1 5/2005 Culum et al.
2005/0105734 A1 5/2005 Buer
2005/0108164 A1 5/2005 Salafia et al.
2005/0109836 A1 5/2005 Ben-Aissa
2005/0109841 A1 5/2005 Ryan et al.
2005/0113070 A1 5/2005 Okabe
2005/0114149 A1 5/2005 Rodriguez et al.
2005/0114150 A1 5/2005 Franklin
2005/0116020 A1 6/2005 Smolucha et al.
2005/0119979 A1 6/2005 Murashita et al.
2005/0124294 A1 6/2005 Wentink
2005/0138390 A1 6/2005 Adams et al.
2005/0138576 A1 6/2005 Baumert et al.
2005/0139656 A1 6/2005 Arnouse
2005/0141451 A1 6/2005 Yoon et al.
2005/0152394 A1 7/2005 Cho
2005/0154897 A1 7/2005 Holloway et al.
2005/0169292 A1 8/2005 Young
2005/0180385 A1 8/2005 Jeong et al.
2005/0182661 A1 8/2005 Allard et al.
2005/0182975 A1 8/2005 Guo et al.
2005/0187792 A1 8/2005 Harper
2005/0195975 A1 9/2005 Kawakita
2005/0200453 A1 9/2005 Turner
2005/0201389 A1 9/2005 Shimanuki et al.
2005/0210270 A1 9/2005 Rohatgi et al.
2005/0212657 A1* 9/2005 Simon G06F 21/32 340/5.74
2005/0215233 A1 9/2005 Perera et al.
2005/0216313 A1 9/2005 Claud et al.
2005/0216639 A1 9/2005 Sparer et al.
2005/0220046 A1 10/2005 Falck et al.
2005/0229007 A1 10/2005 Bolle et al.
2005/0229240 A1 10/2005 Nanba
2005/0242921 A1 11/2005 Zimmerman et al.
2005/0243787 A1 11/2005 Hong et al.
2005/0251688 A1 11/2005 Nanavati et al.
2005/0253683 A1 11/2005 Lowe
2005/0264416 A1 12/2005 Maurer
2005/0269401 A1 12/2005 Spitzer et al.
2005/0272403 A1 12/2005 Ryu et al.
2005/0281320 A1 12/2005 Neugebauer
2005/0282558 A1 12/2005 Choi et al.
2005/0284932 A1 12/2005 Sukeda et al.
2006/0001525 A1 1/2006 Nitzan et al.
2006/0014430 A1 1/2006 Liang et al.
2006/0022042 A1 2/2006 Smets et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0022046 A1 2/2006 Iwamura
2006/0022800 A1 2/2006 Krishna et al.
2006/0025180 A1 2/2006 Rajkotia et al.
2006/0026673 A1 2/2006 Tsuchida
2006/0030353 A1 2/2006 Jun
2006/0034250 A1 2/2006 Kim et al.
2006/0041746 A1 2/2006 Kirkup et al.
2006/0058102 A1 3/2006 Nguyen et al.
2006/0063575 A1 3/2006 Gatto et al.
2006/0069814 A1 3/2006 Abraham et al.
2006/0072586 A1 4/2006 Callaway, Jr. et al.
2006/0074713 A1 4/2006 Conry et al.
2006/0076401 A1 4/2006 Frerking
2006/0078176 A1 4/2006 Abiko et al.
2006/0087407 A1 4/2006 Stewart et al.
2006/0089138 A1 4/2006 Smith et al.
2006/0097949 A1 5/2006 Luebke et al.
2006/0111955 A1 5/2006 Winter et al.
2006/0113381 A1 6/2006 Hochstein et al.
2006/0136728 A1 6/2006 Gentry et al.
2006/0136742 A1 6/2006 Giobbi
2006/0143441 A1 6/2006 Giobbi
2006/0144943 A1 7/2006 Kim
2006/0156027 A1 7/2006 Blake
2006/0158308 A1 7/2006 McMullen et al.
2006/0165060 A1 7/2006 Dua
2006/0170565 A1 8/2006 Husak et al.
2006/0173991 A1 8/2006 Piikivi
2006/0187029 A1 8/2006 Thomas
2006/0190348 A1 8/2006 Ofer et al.
2006/0190413 A1 8/2006 Harper
2006/0194598 A1 8/2006 Kim et al.
2006/0195576 A1 8/2006 Rinne et al.
2006/0198337 A1 9/2006 Hoang et al.
2006/0205408 A1 9/2006 Nakagawa et al.
2006/0208066 A1 9/2006 Finn et al.
2006/0208853 A1 9/2006 Kung et al.
2006/0222042 A1 10/2006 Teramura et al.
2006/0229909 A1 10/2006 Kaila et al.
2006/0237528 A1 10/2006 Bishop et al.
2006/0238305 A1 10/2006 Loving et al.
2006/0268891 A1 11/2006 Heidari-Bateni et al.
2006/0273176 A1 12/2006 Audebert et al.
2006/0274711 A1 12/2006 Nelson, Jr. et al.
2006/0279412 A1 12/2006 Holland et al.
2006/0286969 A1 12/2006 Talmor et al.
2006/0290580 A1 12/2006 Noro et al.
2006/0293925 A1 12/2006 Flom
2006/0294388 A1 12/2006 Abraham et al.
2007/0005403 A1 1/2007 Kennedy et al.
2007/0007331 A1 1/2007 Jasper et al.
2007/0008070 A1 1/2007 Friedrich
2007/0008916 A1 1/2007 Haugli et al.
2007/0016800 A1 1/2007 Spottswood et al.
2007/0019845 A1 1/2007 Kato
2007/0029381 A1 2/2007 Braiman
2007/0032288 A1 2/2007 Nelson et al.
2007/0033072 A1 2/2007 Bildirici
2007/0033150 A1 2/2007 Nwosu
2007/0038751 A1 2/2007 Jorgensen
2007/0050259 A1 3/2007 Wesley
2007/0060095 A1 3/2007 Subrahmanya et al.
2007/0060319 A1 3/2007 Block et al.
2007/0064742 A1 3/2007 Shvodian
2007/0069852 A1 3/2007 Mo et al.
2007/0072636 A1 3/2007 Worfolk et al.
2007/0073553 A1 3/2007 Flinn et al.
2007/0084523 A1 4/2007 McLean
2007/0087682 A1 4/2007 DaCosta
2007/0087834 A1 4/2007 Moser et al.
2007/0100939 A1 5/2007 Bagley et al.
2007/0109117 A1 5/2007 Heitzmann et al.
2007/0112676 A1 5/2007 Kontio et al.
2007/0118891 A1 5/2007 Buer
2007/0133478 A1 6/2007 Armbruster et al.
2007/0136407 A1 6/2007 Rudelic
2007/0152826 A1 7/2007 August et al.
2007/0156850 A1 7/2007 Corrion
2007/0158411 A1 7/2007 Krieg, Jr.
2007/0159301 A1 7/2007 Hirt et al.
2007/0159994 A1 7/2007 Brown et al.
2007/0169121 A1 7/2007 Hunt et al.
2007/0174809 A1 7/2007 Brown et al.
2007/0176756 A1 8/2007 Friedrich
2007/0187266 A1 8/2007 Porter et al.
2007/0192601 A1 8/2007 Spain et al.
2007/0194882 A1 8/2007 Yokota et al.
2007/0204078 A1 8/2007 Boccon-Gibod et al.
2007/0205860 A1 9/2007 Jones et al.
2007/0205861 A1 9/2007 Nair et al.
2007/0213048 A1 9/2007 Trauberg
2007/0214492 A1 9/2007 Gopi et al.
2007/0218921 A1 9/2007 Lee et al.
2007/0219926 A1 9/2007 Korn
2007/0220272 A1 9/2007 Campisi et al.
2007/0229268 A1 10/2007 Swan et al.
2007/0245157 A1 10/2007 Giobbi et al.
2007/0245158 A1 10/2007 Giobbi et al.
2007/0247366 A1 10/2007 Smith et al.
2007/0260883 A1 11/2007 Giobbi et al.
2007/0260888 A1 11/2007 Giobbi et al.
2007/0266257 A1 11/2007 Camaisa et al.
2007/0268862 A1 11/2007 Singh et al.
2007/0271194 A1 11/2007 Walker et al.
2007/0271433 A1 11/2007 Takemura
2007/0277044 A1 11/2007 Graf et al.
2007/0285212 A1 12/2007 Rotzoll
2007/0285238 A1 12/2007 Batra
2007/0288263 A1 12/2007 Rodgers
2007/0288752 A1 12/2007 Chan
2007/0293155 A1 12/2007 Liao et al.
2007/0294755 A1 12/2007 Dadhia et al.
2007/0296544 A1 12/2007 Beenau et al.
2008/0001783 A1 1/2008 Cargonja et al.
2008/0005432 A1 1/2008 Kagawa
2008/0008359 A1 1/2008 Beenau et al.
2008/0011842 A1 1/2008 Curry et al.
2008/0012685 A1 1/2008 Friedrich et al.
2008/0012767 A1 1/2008 Caliri et al.
2008/0016004 A1 1/2008 Kurasaki et al.
2008/0019578 A1 1/2008 Saito et al.
2008/0028453 A1 1/2008 Nguyen et al.
2008/0046715 A1 2/2008 Balazs et al.
2008/0061941 A1 3/2008 Fischer et al.
2008/0071577 A1 3/2008 Highley
2008/0072063 A1 3/2008 Takahashi et al.
2008/0088475 A1 4/2008 Martin
2008/0090548 A1 4/2008 Ramalingam
2008/0095359 A1 4/2008 Schreyer et al.
2008/0109895 A1 5/2008 Janevski
2008/0111752 A1 5/2008 Lindackers et al.
2008/0129450 A1 6/2008 Riegebauer
2008/0148351 A1 6/2008 Bhatia et al.
2008/0149705 A1 6/2008 Giobbi et al.
2008/0150678 A1 6/2008 Giobbi et al.
2008/0156866 A1 7/2008 McNeal
2008/0164997 A1 7/2008 Aritsuka et al.
2008/0169909 A1 7/2008 Park et al.
2008/0186166 A1 8/2008 Zhou et al.
2008/0188308 A1 8/2008 Shepherd et al.
2008/0201768 A1 8/2008 Koo et al.
2008/0209571 A1 8/2008 Bhaskar et al.
2008/0218416 A1 9/2008 Handy et al.
2008/0222701 A1 9/2008 Saaranen et al.
2008/0228524 A1 9/2008 Brown
2008/0235144 A1 9/2008 Phillips
2008/0238625 A1 10/2008 Rofougaran et al.
2008/0250388 A1 10/2008 Meyer et al.
2008/0251579 A1 10/2008 Larsen
2008/0278325 A1 11/2008 Zimman et al.
2008/0289032 A1 11/2008 Aoki et al.
2008/0313728 A1 12/2008 Pandrangi et al.
2008/0314971 A1 12/2008 Faith et al.
2008/0316045 A1 12/2008 Sriharto et al.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2009/0002134	A1	1/2009	McAllister
2009/0016573	A1	1/2009	McAfee, II et al.
2009/0024584	A1	1/2009	Dharap et al.
2009/0033464	A1	2/2009	Friedrich
2009/0033485	A1	2/2009	Naeve et al.
2009/0036164	A1	2/2009	Rowley
2009/0045916	A1	2/2009	Nitzan et al.
2009/0052389	A1	2/2009	Qin et al.
2009/0076849	A1	3/2009	Diller
2009/0081996	A1	3/2009	Duggal et al.
2009/0096580	A1	4/2009	Paananen
2009/0140045	A1	6/2009	Evans
2009/0157512	A1	6/2009	King
2009/0176566	A1	7/2009	Kelly
2009/0199206	A1	8/2009	Finkenzeller et al.
2009/0237245	A1	9/2009	Brinton et al.
2009/0237253	A1	9/2009	Neuwirth
2009/0239667	A1	9/2009	Rowe et al.
2009/0310514	A1	12/2009	Jeon et al.
2009/0313689	A1	12/2009	Nystrom et al.
2009/0319788	A1	12/2009	Zick et al.
2009/0320118	A1	12/2009	Muller et al.
2009/0322510	A1	12/2009	Berger et al.
2009/0328182	A1	12/2009	Malakapalli et al.
2010/0007498	A1	1/2010	Jackson
2010/0023074	A1	1/2010	Powers et al.
2010/0037255	A1	2/2010	Sheehan et al.
2010/0077214	A1	3/2010	Jogand-Coulomb et al.
2010/0117794	A1	5/2010	Adams et al.
2010/0134257	A1	6/2010	Puleston et al.
2010/0169442	A1	7/2010	Liu et al.
2010/0169964	A1	7/2010	Liu et al.
2010/0174911	A1	7/2010	Isshiki
2010/0188226	A1	7/2010	Seder et al.
2010/0277283	A1	11/2010	Burkart et al.
2010/0277286	A1	11/2010	Burkart et al.
2010/0291896	A1	11/2010	Corda
2010/0305843	A1	12/2010	Yan et al.
2010/0328033	A1	12/2010	Kamei
2011/0072034	A1	3/2011	Sly et al.
2011/0072132	A1	3/2011	Shafer et al.
2011/0082735	A1	4/2011	Kannan et al.
2011/0116358	A9	5/2011	Li et al.
2011/0126188	A1	5/2011	Bernstein et al.
2011/0227740	A1	9/2011	Wohltjen
2011/0238517	A1	9/2011	Ramalingam et al.
2011/0246790	A1	10/2011	Koh et al.
2011/0266348	A1	11/2011	Denniston, Jr.
2011/0307599	A1	12/2011	Saretto et al.
2012/0086571	A1	4/2012	Scalisi et al.
2012/0182123	A1	7/2012	Butler et al.
2012/0212322	A1	8/2012	Idsoe
2012/0226907	A1	9/2012	Hohberger
2013/0019295	A1	1/2013	Park et al.
2013/0019323	A1	1/2013	Arvidsson et al.
2013/0044111	A1	2/2013	VanGilder et al.
2013/0111543	A1	5/2013	Brown et al.
2013/0276140	A1	10/2013	Coffing et al.
2013/0331063	A1	12/2013	Cormier et al.
2014/0074696	A1	3/2014	Glaser
2014/0266713	A1	9/2014	Sehgal et al.
2016/0210614	A1	7/2016	Hall
2017/0085564	A1	3/2017	Giobbi et al.

FOREIGN PATENT DOCUMENTS

WO	0122724	A1	3/2001
WO	0135334	A1	5/2001
WO	0175876	A1	10/2001
WO	0177790	A1	10/2001
WO	05050450		10/2001
WO	05086802		10/2001
WO	2004/038563		5/2004
WO	2007/087558		8/2007

OTHER PUBLICATIONS

"Geetha Govindan, Suresh Kumar Bakakrishnan, Rejith Lalitha Ratheendran, Saji Koyippurathu Sivadasan, Real time security management using RFID, Biometric and Smart Messages, Aug. 20-22, 2009, IEEE Xplore, INSPEC # 10906130" (Year: 2009).*

"Sweta Singh, Akhilesh Singh, Rakesh Kumar, A constraint-based biometric scheme on ATM and swiping machine, Mar. 11-13, 2016, IEEE Xplore, INSPEC $ 16156324" (Year: 2016).*

Vainio, Juha., "Bluetooth Security", dated 2000, Helskinki University of Technology, p. 1-20.

Katz et al., "Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification System", dated 2002, Smart Card Alliance, p. 1-29.

Dai et al., "Toward Blockchain-Based Accounting and Assurance", 2017, Journal of Information Systems, pp. 5-21 (Year: 2017).

Alliance Activities: Publications: Identity-Smart Card Alliance, Smart Card Alliance, 1997-2007, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet, https://www.smartcardalliance.org/pages/publications-identity.

Antonoff, Michael, Visiting Video Valley, Sound Vision, pp. 116 and 118-119, Nov. 2001.

Applying Biometrics to Door Access, Security Magazine, Sep. 26, 2002 [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.securitymagazine.com/CDA/Articles/Technologies/3ae610eaa34d8010VgnVCM100000f932a8c0.

BioPay, LLC, Frequently Asked Questions (FAQs) About BioPay, BioPay, LLC, 2007, [online] [Retrieved on Jan. 1, 2007] Retrieved from the Internet http://www.biopay.com/faqs-lowes.asp.

Bluetooth, www.bluetoothcom, Printed Jlllle l, 2000.

Blum, Jonathan , Digital Rights Managment May Solve The Napster Problem, Technoloav Investor Industrvsector (Oct. 2000),24-27.

Content protection plan targets wireless home networks, www.eetimes.com, Jan. 11, 2002.

Debow, Credit/Debit Debuts in Midwest Smart Card Test, Computers in Banking, v6, n11, p. 10, Nov. 1989.

Dennis, Digital Passports Need Not Infringe Civil Liberties, Newsbytes, Dec. 2, 1999, 2 pages.

Farouk, Authentication Mechanisms in Grid Computing Environment Comparative Study, 2012, IEEE, p. 1-6.

Fasca, Chad. The Circuit, Electronic News 45(45). (Nov. 8, 1999),20.

Firecrest Shows How Truly Commercially-Minded Companies Will Exploit the Internet, Computergram International, Jan. 18, 1996. 2pgs.

Kontzer, Tony , Thomson Bets on Smart Cards for Video Encryption, www.informationweek.com, Jun. 7, 2001 (Also listed under Press Release).

Lake, Matt. Downloading for Dollars, Sound Vision. (Nov. 2000),137-138.

Lewis, Sony and Visa in On-Line Entertainment Venture, New York Times, v145, Nov. 16, 1995. 1 pg.

Liu et al. 2001. A Practical Guide to Biometric Security Technology. IT Professional 3, 1 (Jan. 2001), 27-32. DOI=10.1109/6294_899930 http://dx.doi.org/10.1109/6294.899930.

McIver, R. et al., Identification and Verification Working Together, BioscryptTM, Aug. 27, 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.ibia.org/membersadmin/whitepapers/pdf/15/Identification%20and%20Verification%20Working%20Together.pdf.

Micronas and Thomson multimedia Showcase a New Copy Protection System That Will Drive the Future of Digital Television, www.micronas.com, Jan. 8, 2002.

Nilsson, J. et al., Match-On-Card for Java Cards, Precise Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20for%20Java%20Cards.pdf.

Nordin, B., Match-On-Card Technology, PreciseTM Biometrics, White Paper, Apr. 2004, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf.

(56) **References Cited**

OTHER PUBLICATIONS

Paget, Paul, The Security Behind Secure Extranets, Enterprise Systems Journal, (Dec. 1999), 4 pgs.
PCT International Search Report and Written Opinion, PCT/US04/38124, dated Apr. 7, 2005, 10 pages.
PCT International Search Report and Written Opinion, PCT/US05/07535, dated Dec. 6, 2005, 6 pages.
PCT International Search Report and Written Opinion, PCT/US05/43447, dated Feb. 22, 2007, 7 pages.
PCT International Search Report and Written Opinion, PCT/US05/46843, dated Mar. 1, 2007, 10 pages.
PCT International Search Report and Written Opinion, PCT/US07/11103, dated Apr. 23, 2008, 9 pages.
PCT International Search Report and Written Opinion, PCT/US07/11105, dated Oct. 20, 2008, 10 pages.
PCT International Search Report PCT/US07/11104, Jun. 26, 2008, 9 pages.
PCT International Search Report, PCT/US07/11102, dated Oct. 3, 2008, 11 pages.
Pope, Oasis Digital Signature Services: Digital Signing without the Headaches, Internet Computing IEEE, vol. 10, 2006, pp. 81-84.
SAFModuleTM: A Look Into Strong Authentication, saflink Corporation, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.ibia.org/membersadmin/whitepapers/pdf/6/SAFmod_WP.pdf.
Sapsford, Jathon, E-Business: Sound Waves Could Help Ease Web-Fraud Woes, Wall Street Journal, (Aug. 14, 2000), B1.
Say Hello to Bluetooth, Bluetooth Web site 4 pages.
Smart Card Alliance Report, Contactless Technology for Secure Physical Access: Technology and Standsards Choices, Smart Card Alliance, Oct. 2002, p. 1-48.
Smart Cards and Biometrics White Paper, Smart Card Alliance, May 2002, [online] [Retrieved on Jan. 7, 2007] Retrieved from the Internet http://www.securitymanagement.com/library/smartcard_faqtech0802.pdf.
Thomson multimedia unveils copy protection proposal designed to provide additional layer of digital content security, www.thomson-multimedia.com, May 30, 2001. 2 pgs.
Van Winkle, William, Bluetooth the King of Connectivity, Laptop Buyers Guide and Handbook (Jan. 2000), 148-153.
Wade, W., Using Fingerprints to Make Payments at POS Slowly Gaining Popularity, Credit Union Journal, International Biometric Group, Apr. 21, 2003, online. Retrieved on Jan. 7, 2007. http://www.biometricgroup.com/in_the_news/04.21.03.html.
Wallace, Bob, The Internet Unplugged, InformationWeek, 765(22), (Dec. 13, 1999), 22-24.
Weber, Thomas E., In the Age of Napster, Protecting Copyright is a Digital Arms Race, Wall Street Journal, (Jul. 24, 2000), B1.
What is a File, Apr. 30, 1998, http://unixhelp.ed.ac.uk/editors/whatisafile.html.accessed Mar. 11, 2010 via http://waybackmachine.org/19980615000000*/http://unixhelp.ed.ac.uk/editors/whatisafile.html.
Yoshida, Junko, Content Protection Plan Targets Wireless Home Networks, www.eetimes.com, Jan. 11, 2002, 2 pgs.
Chen, et al. "On Enhancing Biometric Authentication with Data Protection." KES2000. Fourth International Conference on Knowledge-Based Intelligent Engineering Systems and Allied Technologies. Proceedings (Cat. No. 00TH8516), vol. 1, 2000, pp. 249-252 vol. 1.
Noore, A. "Highly Robust Biometric Smart Card Design." IEEE Transactions on Consumer Electronics, vol. 46, No. 4, 2000, pp. 1059-1063.
Anonymous, "Applying Biometrics to Door Access," Security Magazine, Sep. 26, 2002, retrieved from http://www.securitymagazine.com/CDA/Articles/Technologies/3ae610eaa34d8010VgnVCM100000f932a8c0___ on Jan. 7, 2007, 5 pgs.
Anonymous, "IEEE 802.15.4-2006—Wikipedia, the free encyclopedia," Wikipedia, last modified Mar. 21, 2009, retrieved from http://en.wikipedia.org/wiki/IEEE_802.15.4-2006 on Apr. 30, 2009, 5 pgs.
Apple et al., "Smart Card Setup Guide," 2006, downloaded from http://manuals.info.apple.com/en_US/Smart_Card_Setup_Guide.pdf on or before May 3, 2012, 16 pgs.
Balanis, "Antenna Theory: A Review," Jan. 1992, Proceedings of the IEEE, vol. 80, No. 1, p. 13.
Beaufour, "Personal Servers as Digital Keys," Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications (PERCOM'04), Mar. 14-17, 2004, pp. 319-328.
Blueproximity, "BlueProximity—Leave it—it's locked, come back, it's back too . . . " Aug. 26, 2007, retrieved from http://blueproximity.sourceforge.net/ via http://www.archive.org/ on or before Oct. 11, 2011, 1 pg.
Bohrsatom et al., "Automatically unlock PC when entering proximity," Dec. 7, 2005, retrieved from http://salling.com/forums/viewtopic.php?t=3190 on or before Oct. 11, 2011, 3 pgs.
Brown, "Techniques for Privacy and Authentication in Personal Communication Systems," Personal Communications, IEEE, Aug. 1995, vol. 2, No. 4, pp. 6-10.
Cisco Systems, Inc., "Antenna Patterns and Their Meaning," 1992-2007, p. 10.
Costa, "Imation USB 2.0 Micro Hard Drive," Nov. 22, 2005, retrieved from http://www.pcmag.com/article2/0,2817,1892209,00.asp on or before Oct. 11, 2011, 2 pgs.
Dagan, "Power over Ethernet (PoE) Midspan—The Smart Path to Providign Power for IP Telephony," Product Manager, Systems, Aug. 2005, Power Dsine Inc., 28 pgs.
Derfler, "How Networks Work," Bestseller Edition, 1996, Ziff-Davis Press, Emeryville, CA, all pages.
Giobbi, Specification of U.S. Appl. No. 60/824,758, filed Sep. 6, 2006, all pages.
Gralla, "How the Internet Works," Millennium Edition, 1999, Que Corporation, Indianapolis, IN, all pages.
Hendron, "File Security, Keychains, Encryptioin, and More with Mac OS X (10.3+)" Apr. 4, 2005, downloaded from http://www.johnhendron.net/documents/OSX_Security.pdf on or before May 3, 2012, 30 pgs.
International Search Report and Written Opinion for International Application No. PCT/US07/00349, dated Mar. 19, 2008, 10 pgs.
International Search Report and Written Opinion for International Application No. PCT/US08/83060, dated Dec. 29, 2008, 9 pgs.
International Search Report and Written Opinion for International Application No. PCT/US08/87835, dated Feb. 11, 2009, 8 pgs.
International Search Report and Written Opinion for International Application No. PCT/US09/34095, dated Mar. 25, 2009, 11 pgs.
International Search Report and Written Opinion for International Application No. PCT/US2009/039943, dated Jun. 1, 2009, 9 pgs.
International Search Report and Written Opinion for International Application No. PCT/US2014/037609, dated Dec. 9, 2014, 13 pgs.
Lee et al., "Effects of dielectric superstrates on a two-layer electromagnetically coupled patch antenna," Antennas and Propagation Society International Symposium, Jun. 1989, AP-S. Digest, vol. 2, pp. 26-30, found at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1347.
Muller, "Desktop Encyclopedia of the Internet," 1999, Artech House Inc., Norwood, MA, all pages.
National Criminal Justice Reference Service, "Antenna Types," Dec. 11, 2006, online at http://ncjrs.gov/pdffiles1/nij/185030b.pdf, retrieved from http://web.archive.org/web/*/http://www.ncjrs.gov/pdffiles1/nij/185030b.pdf on Jan. 12, 2011, 1 pg.
Nel et al., "Generation of Keys for use with the Digital Signature Standard (DSS)," Communications and Signal Processing, Proceedings of the 1993 IEEE South African Symposium, Aug. 6, 1993, pp. 6-11.
Nerd Vittles, "magicJack: Could It Be the Asterisk Killer?" Aug. 1, 2007, retrieved from http://nerdvittles.com/index.php?p=187 on or before Oct. 11, 2011, 2 pgs.
Nordin, "Match-on-Card Technology," Precise Biometrics, white paper, Apr. 2004, retrieved from www.ibia.org/membersadmin/whitepapers/pdf/17/Precise%20Match-on-Card%20technology.pdf on Jan. 7, 2007, 7 pgs.

(56) **References Cited**

OTHER PUBLICATIONS

Pash, "Automate proximity and location-based computer actions," Jun. 5, 2007, retrieved from http://lifehacker.com/265822/automate-proximity-and-location+based-computer-actions on or before Oct. 11, 2011, 3 pgs.
SplashID, "SplashID—Secure Password Manager for PDAs and Smartphones," Mar. 8, 2007, retrieved from http://www.splashdata.com/splashid/ via http://www.archive.org/ on or before Oct. 11, 2011, 2 pgs.
Srivastava, "Is Internet security a major issue with respect to the slow acceptance rate of digital signatures," Jan. 2, 2005, Computer Law & Security Report, pp. 392-404.
White, "How computers Work," Millennium Edition, 1999, Que Corporation, Indianapolis, IN, all pages.

* cited by examiner

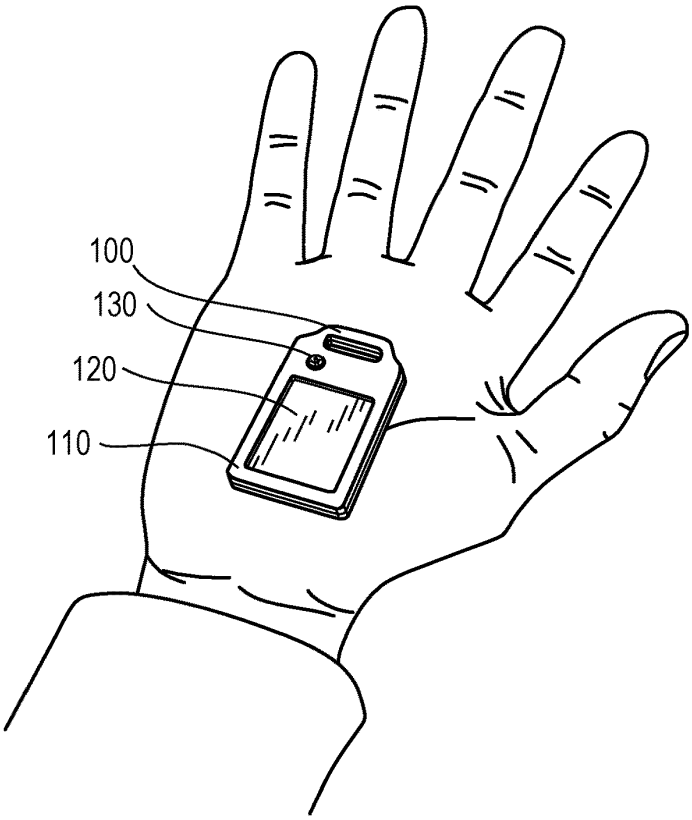

100
130
120
110

FIG. 1

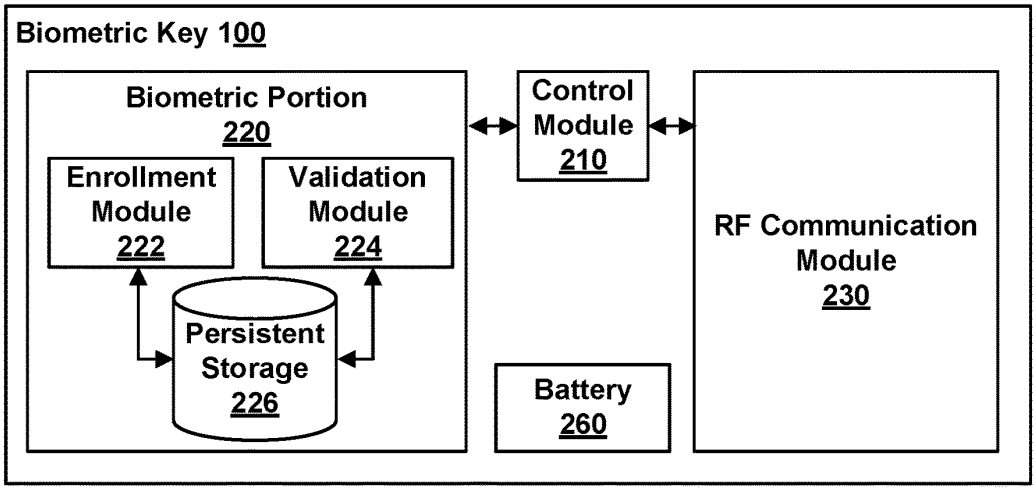

Biometric Key 100
Biometric Portion 220
Enrollment Module 222
Validation Module 224
Persistent Storage 226
Control Module 210
Battery 260
RF Communication Module 230

FIG. 2

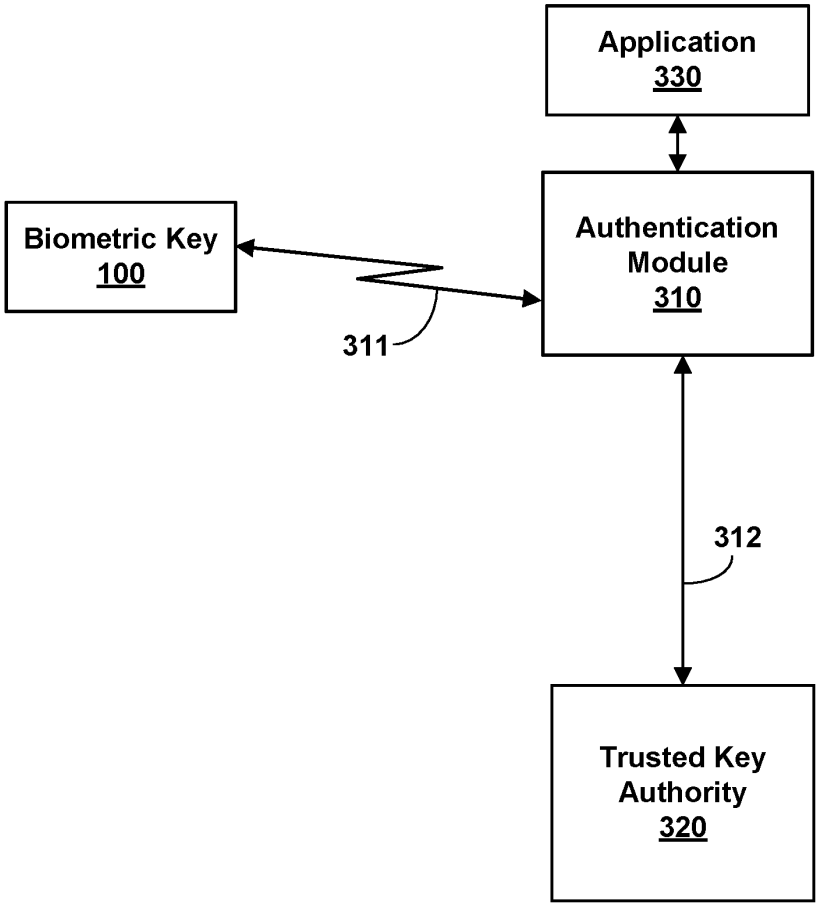

Application
330
Biometric Key
100
Authentication
Module
310
311
312
Trusted Key
Authority
320

FIG. 3

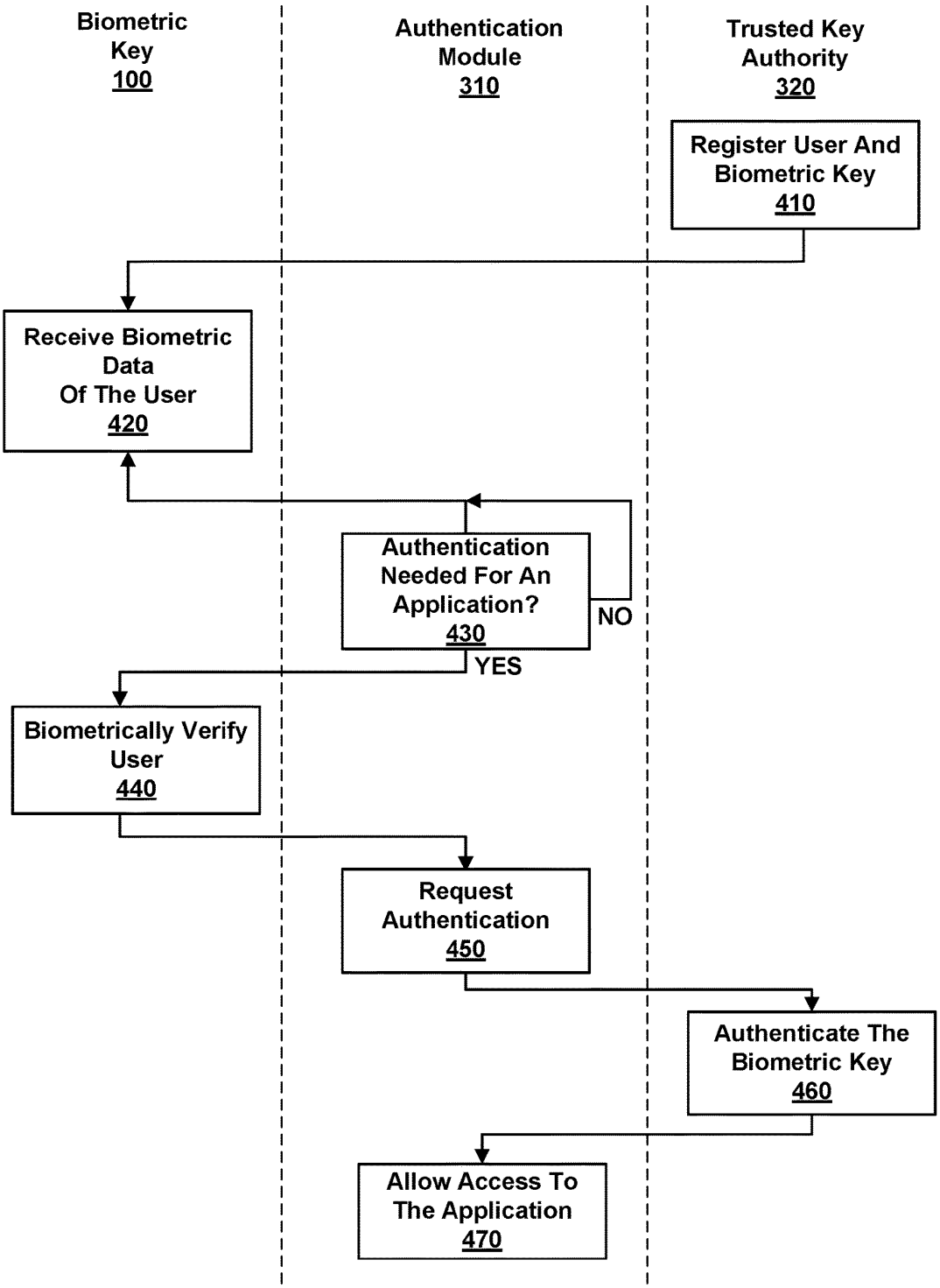

Biometric Key 100
Authentication Module 310
Trusted Key Authority 320
Register User And Biometric Key 410
Receive Biometric Data Of The User 420
Authentication Needed For An Application? 430
NO
YES
Biometrically Verify User 440
Request Authentication 450
Authenticate The Biometric Key 460
Allow Access To The Application 470

FIG. 4

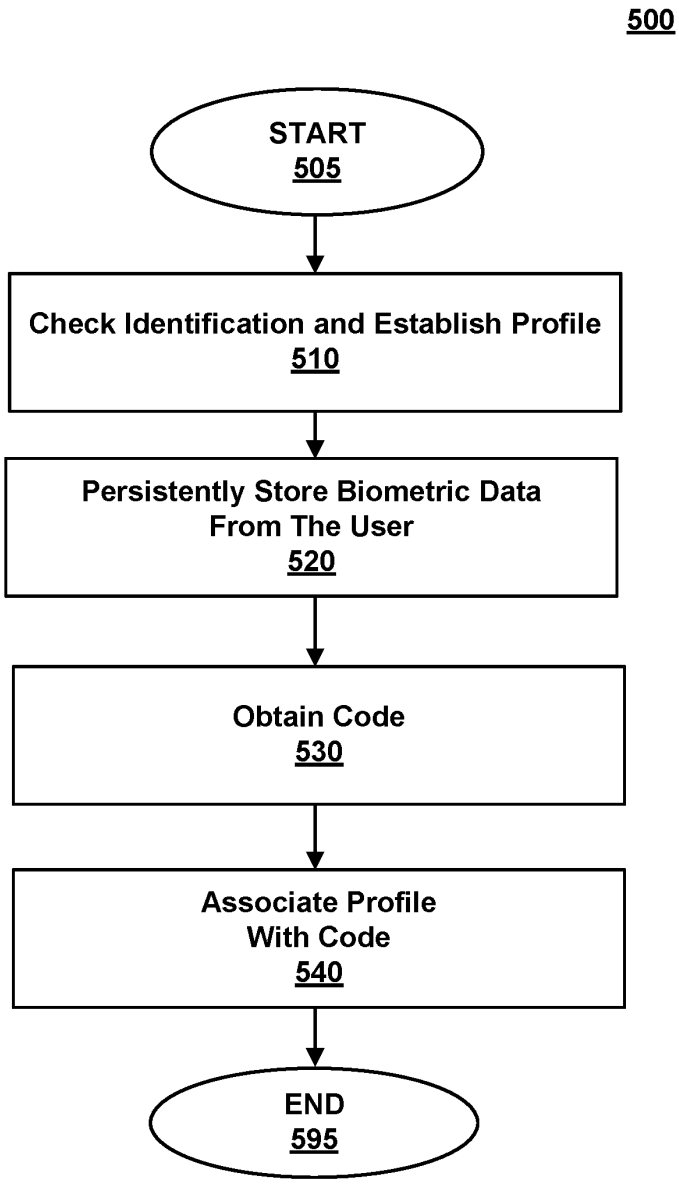

500
START
505
Check Identification and Establish Profile
510
Persistently Store Biometric Data
From The User
520
Obtain Code
530
Associate Profile
With Code
540
END
595

FIG. 5

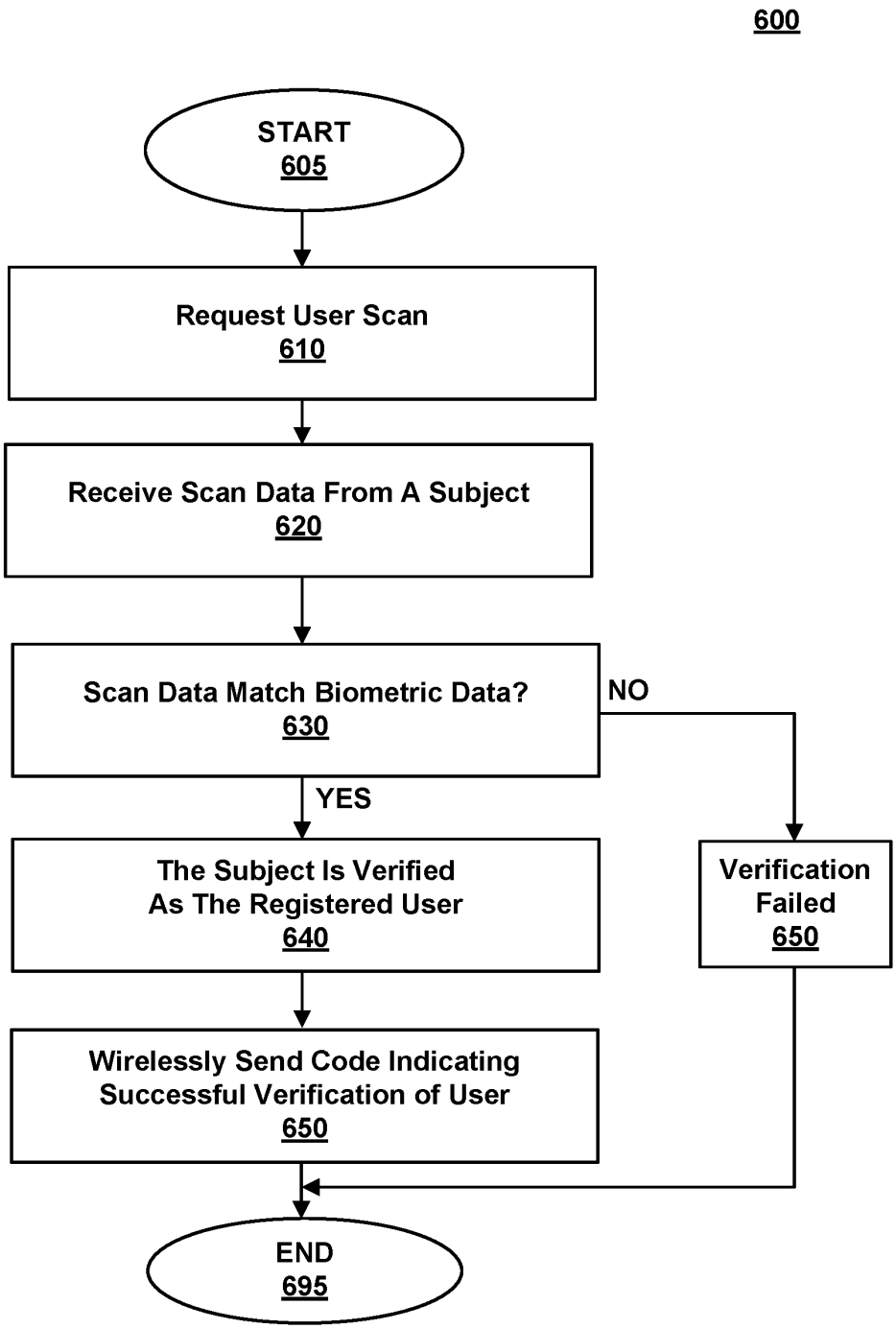

600
START
605
Request User Scan
610
Receive Scan Data From A Subject
620
Scan Data Match Biometric Data?
630
NO
YES
The Subject Is Verified
As The Registered User
640
Verification
Failed
650
Wirelessly Send Code Indicating
Successful Verification of User
650
END
695

FIG. 6

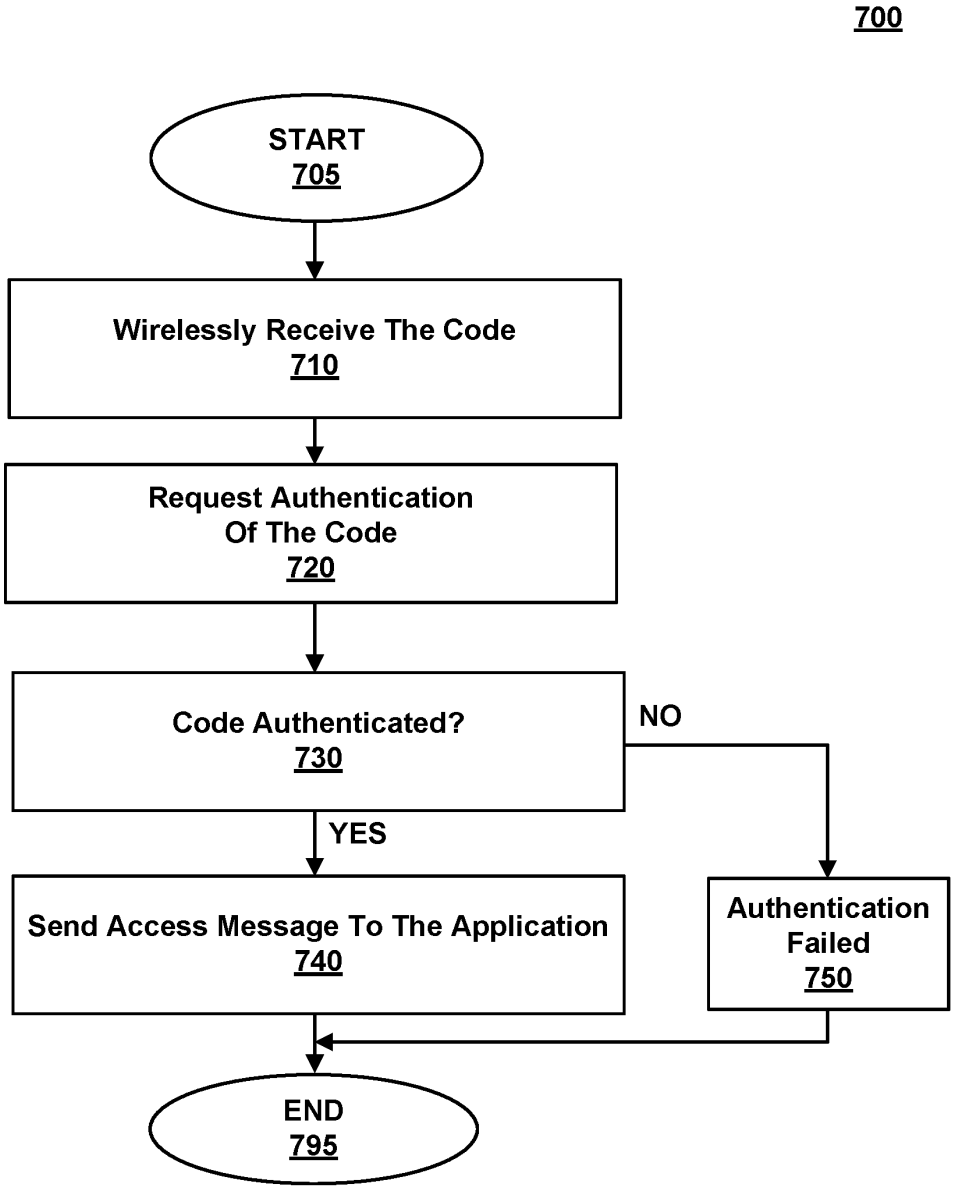

700
START
705
Wirelessly Receive The Code
710
Request Authentication
Of The Code
720
Code Authenticated?
730
NO
YES
Send Access Message To The Application
740
Authentication
Failed
750
END
795

FIG. 7

BIOMETRIC PERSONAL DATA KEY (PDK) AUTHENTICATION

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority, under 35 U.S.C. § 120, to U.S. patent application Ser. No. 14/521,982, filed Oct. 23, 2014, entitled "Biometric Personal Data Key (PDK) Authentication, which claims priority to U.S. patent application Ser. No. 13/710,109 filed Dec. 10, 2012 and entitled "Biometric Personal Data Key (PDK) Authentication" which claims priority to U.S. patent application Ser. No. 11/314,199, filed Dec. 20, 2005 and entitled "Biometric Personal Data Key (PDK) Authentication," which claims the benefit of U.S. Provisional Application No. 60/637,538, filed on Dec. 20, 2004, and of U.S. Provisional Application No. 60/652,765, filed on Feb. 14, 2005, the entireties of which are hereby incorporated by reference.

Applicants hereby notify the USPTO that the claims of the present application are different from those of the aforementioned related applications. Therefore, Applicant rescinds any disclaimer of claim scope made in the parent application or any other predecessor application in relation to the present application. The Examiner is therefore advised that any such disclaimer and the cited reference that it was made to avoid may need to be revisited at this time. Furthermore, the Examiner is also reminded that any disclaimer made in the present application should not be read into or against the parent application, the grandparent application or any other related application.

FIELD OF THE INVENTION

The present invention relates generally to computerized authentication, and more specifically, to an authentication responsive to biometric verification of a user being authenticated.

BACKGROUND

Conventional user authentication techniques are designed to prevent access by unauthorized users. One technique is to require a user being authenticated to provide secret credentials, such as a password, before allowing access. Similarly, a PIN number can be required by an ATM machine before allowing a person to perform automated bank transactions. A difficulty with this technique is that it requires the user to memorize or otherwise keep track of the credentials. A uses often has multiple sets of credentials (e.g., passwords and PINs) and it can be quite difficult to keep track of them all.

Another technique that does not require the user to memorize credentials is to provide the user with an access object such as a key (e.g., an electronic key) that the user can present to obtain access. For example, a user can be provided with a small electronic key fob that allows access to a building or other secured location. A difficulty with using access objects is that authentication merely proves that the access object itself is valid; it does not verify that the legitimate user is using the access object. That is, illegitimate user can use a stolen access object to enter a secured location because the user's identity is never checked.

Some hybrid authentication techniques require the user to provide both an access object and credentials. The user is authenticated only upon providing both items. Of course, this solution does not resolve the problem of making the user memorize credentials.

Therefore, there is a need for systems and methods for verifying a user that is being authenticated that does not suffer from the limitations described above. Moreover, the solution should ease authentications by wirelessly providing an identification of the user.

SUMMARY

The present invention addresses the above needs by providing systems and methods for authentication responsive to biometric verification of a user being authenticated. In one embodiment, an integrated device includes a persistent storage to persistently stores a code such as a device identifier (ID) and biometric data for a user in a tamper-resistant format, and a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending a code for authentication.

In one embodiment, a method for verifying a user during authentication of an integrated device, includes persistently storing biometric data for the user in a tamper-resistant format; responsive to receiving a request for biometric verification of the user, receiving scan data from a biometric scan; comparing the scan data to the biometric data to determine whether the data match; and responsive to a determination that the scan data matches the biometric data, wirelessly sending a code for authentication.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance the operations further include registering an age verification for the user in association with the code. For instance the operations further include establishing a secure communication channel prior to sending the code for authentication. For instance the operations further include receiving a request for the code without a request for biometric verification, and responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data. For instance, the features include: the code is registered with a trusted authority, and the code can be authenticated to a third party by the trusted authority; the code uniquely identifies the integrated device; the code indicates that the biometric verification was successful; persistently storing biometric data includes permanently storing biometric data; the biometric data and the scan data are both based on a fingerprint scan by the user, an LED to be activated for requesting the biometric scan.

In one embodiment, a method for authenticating a verified user, includes receiving a code associated with a biometrically verified user; requesting authentication of the code; receiving an authentication result; and in response to the authentication result being positive, providing access to an application.

In one embodiment, a system includes an integrated device (e.g. a biometric key) to store biometric data for a user in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending a code; and an authentication module to receive the code and send the code to a trusted authority for authentication, and responsive to the code being authenticated, allowing the user to access an application.

Other embodiments include corresponding systems, apparatus, and computer programming products, configured to perform the actions of the methods, encoded on computer storage devices. These and other embodiments may each optionally include one or more of the following features. For instance, the operations further include registering the code with a trusted authority, wherein requesting authentication of the code includes providing the code to the trusted authority and wherein receiving an authentication result comprises receiving the authentication result from the trusted authority. For instance the operations further include registering a date of birth or age with the trusted authority. For instance the operations further include establishing a secure communications channel with an integrated device, wherein the code associated with the biometrically verified user is received from the integrated device. For instance the features include: the integrated device receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data; when the integrated device cannot verify the scan data as being from the user, it does not send the code.

Advantageously, user authentication is bolstered with highly reliable biometric verification of the user in an integrated device. Furthermore, a keyless environment relieves authorized users from having to memorize credentials, and of having to physically enter credentials or keys. In addition, the integrated device can be authenticated for an application that is open to the public (i.e., in an open loop system).

The features and advantages described in the specification are not all inclusive and, in particular, many additional features and advantages will be apparent to one of ordinary skill in the art in view of the drawings, specifications, and claims. Moreover, it should be noted that the language used in the specification has been principally selected for readability and instructional purposes and may not have been selected to delineate or circumscribe the inventive matter.

BRIEF DESCRIPTION OF THE DRAWINGS

The teachings of the present invention can be readily understood by considering the following detailed description in conjunction with the accompanying drawings.

FIG. **1** is a schematic diagram illustrating a biometric key for providing authentication information for a biometrically verified user according to one embodiment of the present invention.

FIG. **2** is a block diagram illustrating functional modules within the biometric key according to one embodiment of the present invention.

FIG. **3** is a block diagram illustrating a system for providing authentication information for a biometrically verified user.

FIG. **4** is a flow chart illustrating a method for providing authentication information for a biometrically verified user.

FIG. **5** is a flow chart illustrating a method for enrolling biometric data of the user with the biometric key.

FIG. **6** is a flow chart illustrating a method for verifying a subject presenting the biometric key according to one embodiment of the present invention.

FIG. **7** is a flow chart illustrating a method for authenticating a verified user of the biometric key according to one embodiment of the present invention.

DETAILED DESCRIPTION

Systems and methods for authentication responsive to biometric verification of a user being authenticated are described. Generally, biometric verification uses biometric data to ensure that the user of, for example, a biometric key, is the person registered as an owner. Biometric data is a digital or analog representation of characteristics unique to the user's body. For example, a fingerprint of a subject can be compared against previously-recorded biometric data for verification that the subject is the registered owner of the biometric key. Then, the biometric key itself can be authenticated.

Although the embodiments below are described using the example of biometric verification using a fingerprint, other embodiments within the spirit of the present invention can perform biometric verification using other types of biometric data. For example, the biometric data can include a palm print, a retinal scan, an iris scan, hand geometry recognition, facial recognition, signature recognition, or voice recognition.

FIG. **1** is a schematic diagram illustrating an example of a biometric key **100** for providing authentication information for a biometrically verified user according to one embodiment of the present invention. In one embodiment, the biometric key **100** comprises a frame **110**, a scan pad **120**, and an LED **130**. In one embodiment, biometric key **100** has a small form factor (e.g., the size of an automobile remote control) such that it can be unobtrusively carried by a user. In one embodiment, the biometric key **100** is integrated into another object or device. A device having an integrated biometric key **100** is occasionally referred to herein as an "integrated device." For example, in one embodiment, the biometric key **100** is integrated into a mobile phone (e.g. a cellular phone or smartphone), tablet, laptop, mp3 player, mobile gaming device, watch, key fob or other mobile device, thereby making the biometric key **100** unobtrusive to carry.

Frame **110** can be formed by plastic, metal or another suitable material. Frame **110** is shaped to secure scan pad **120**, and includes a perforation for attachment to, for example a key chain or clip. In one embodiment, frame **110** is formed from a unitary molding to protect biometric data. Accordingly, frame **110** cannot be opened to expose the underlying components unless it is broken.

Scan pad **120** can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad **120** can be sized to fit a thumb or other finger. Biometric key **100** of the present embodiment includes LED **130** that lights up to request a fingerprint scan from a user. In one embodiment, LED **130** can also confirm that user verification and/or authentication has completed.

Biometric key **100** can authenticate a user for various purposes. For example, biometric key **100** can allow keyless entry into homes and autos. In another example, biometric key **100** can log a user onto a computer system or point of sale register without typing in credentials. In still another example, biometric key **100** can verify that an enrolled user is above a certain age (e.g., before allowing access to a slot machine in a casino). In some embodiments, biometric key **100** operates without biometric verification, and request a fingerprint scan from a user only when biometric verification is needed for the particular use.

FIG. **2** is a block diagram illustrating biometric key **100** according to one embodiment of the present invention. Biometric key **100** comprises control module **210**, biometric portion **220**, RF communication module **230**, persistent storage **240**, and battery **250**. Biometric key **100** can be formed from a combination of hardware and software components as described above. In one embodiment, biometric key **100** comprises a modified key fob.

Control module **210** coordinates between several functions of biometric key **100**. In one embodiment, control module **210** provides a verification code upon successful verification of the user. More specifically, once biometric portion **220** indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module **210** can trigger RF communication module **230** for sending a code indicating that the user was verified. In another embodiment, control module **210** can work in the opposite direction by detecting a request for verification from RF communication module **230**, and then requesting verification of the user from biometric portion **210**. Note that control module **210** of FIG. **2** is merely a grouping of control functions in a central architecture, and in other embodiments, the control functions can be distributed between several modules around biometric key **100**.

Biometric portion **220** comprises enrollment module **222**, validation module **224**, and biometric data base **226**. In one embodiment, enrollment module **222** registers a user with biometric key **100** by persistently storing biometric data associated with the user. Further, enrollment module **222** registers biometric key **100** with a trusted authority by providing the code (e.g., device ID) to the trusted authority. Or conversely, the trusted authority can provide the code to biometric key **100** to be stored therein.

Validation module **224** can comprise scan pad **120** (FIG. **1**) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module **214** determines whether the user's fingerprint matches the stored biometric data from enrollment. Conventional techniques for comparing fingerprints can be used. For example, the unique pattern of ridges and valleys of the fingerprints can be compared. A statistical model can be used to determine comparison results. Validation module **224** can send comparison results to control module **210**.

In other embodiments, validation module **224** can be configured to capture biometric data for other human characteristics. For example, a digital image of a retina, iris, and/or handwriting sample can be captured. In another example, a microphone can capture a voice sample.

Persistent storage **226** persistently stores biometric data from one or more users which can be provided according to specific implementations. 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** can include, for example, a ROM element, a flash memory element, or any other type of non-volatile storage element. 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.

In one embodiment, persistent storage **226** also stores the code that is provided by the key **100** responsive to successful verification of the user. As described above, in one embodiment the code is a device ID or other value that uniquely identifies biometric key **100**. In one embodiment, the code is providing during the manufacturing process and the biometric data are provided during an enrollment of the user. In other embodiments, the code is provided during enrollment and/or the biometric data are provided during manufacturing. Further, in some embodiments persistent storage **226** stores other data utilized during the operation of biometric key **100**. For example, persistent storage **226** can store encryption/decryption keys utilized to establish secure communications links.

Radio frequency (RF) communication module **230** is, for example, a transceiver or other mechanism for wireless communication. RF communication module **230** can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication **220** can be optimized for low-power usage by, for example, using short-range transceivers. RF communication module **230** can actively send out connection requests, or passively detect connection requests.

Battery **260** can be a conventional power source suitable for the components of biometric key **100**. Battery **260** can be either replaceable or rechargeable. Alternatively, battery **260** can be embedded within key **100** such that the key must be discarded or recycled upon expiration of the battery.

FIG. **3** is a block diagram illustrating a system **300** for providing authentication information for a biometrically verified user. System **300** comprises an authentication module **310** in communication with biometric key **100**, a trusted key authority **320**, and an application **330**.

Authentication module **310** is coupled in communication with biometric key via line **311** (i.e., a wireless medium such as EM signals), and with trusted key authority **320** via line **312** (e.g., a secure data network such as the Internet, or a cell network). Authentication module **310** can include one or more of, for example, a computerized device, software executing on a computerized device, and/or a reader/decoder circuit. In one embodiment, authentication module **310** servers as a gatekeeper to application **330** by requiring the code indicating successful biometric verification of the user prior to allowing access to the application. Further, in one embodiment, authentication module **310** provides the code to trusted key authority **320** in order to verify that it belongs to a legitimate key (e.g., when application **330** is security-critical). 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**.

Application **330** is a resource that can be accessed by a verified and authenticated user. Application **330** can be, for example, a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file, a financial account (e.g. a savings account, checking account, brokerage account, credit card account, credit line, etc.) and the like. In one embodiment, a file includes medical information such as a medical record, insurance information or other healthcare information. Application **330** can execute on the same system as authentication module **310** or on another system in communication with the system of the authentication module. In one embodiment, application module **330** allows access by a user after receiving a message from authentication module **310**. At that point, application **330** can allow direct use by the user, or require that communications continue to pass through authentication module **310** for continued authentication.

Trusted key authority **320** is a third-party authority that is present in some embodiments in order to provide enhanced security. In one embodiment, trusted key authority **320** verifies that a code from a biometric key is legitimate. To do so, the trusted key authority **320** stores a list of codes for legitimate biometric keys. The list can be batched or updated each time a new user/key is enrolled. In one embodiment, trusted key authority **320** can also store a profile associated with a biometric key. The profile describes the user associ-

ated with the key, the key itself, the trusted key authority, and/or other relevant information. In one embodiment, the functionality of trusted key authority **320** is provided by a server or other computerized device.

In an open system, where unknown users can attempt authentication (e.g., in a public grocery store), trusted key authority **320** provides verification that a key presenting a certain code is legitimate. By contrast, in a closed system, only known users are legitimate (e.g., owners of a home), the trusted key authority **320** can be maintained locally and serves to verify that the key belongs to one of the limited number of users that can use the system.

FIG. **4** is a flow chart illustrating a method **400** for authenticating a biometrically verified user using a trusted key authority (e.g., authority **320**). A biometric key (e.g., biometric key **100**) is registered **410** with the trusted key authority. The code (e.g., device ID) of the key is stored by the trusted key authority. Additionally, a user is enrolled **420** with the biometric key as described below with reference to FIG. **5**.

In various situations, authentication of the key is needed **430** (e.g., by authentication module **310**). In one embodiment, authentication can be required prior to allowing access to an application (e.g., application **330**). For example, a user can be standing proximate to a slot machine in a casino which requires that a user be over the age of 21. The slot machine can detect the biometric key in the user's pocket, and, in response, spawn a conspicuous pop-up window on the slot machine requesting age verification. Alternatively, the biometric key can blink an LED. In other embodiments, biometric verification is not necessary and only the key itself is authenticated.

The biometric key establishes communication with the authentication module using various techniques. In one embodiment, the key and authentication module engage in preliminary data exchanges to determine who and/or what they are (e.g., to ascertain that they belong to the same system). These data exchanges can include challenge-response dialogs, hashing algorithms, and the like in order to ensure that the biometric key and authentication module are themselves legitimate. Further, in one embodiment the key and authentication module establish a secure communications channel. The key performs the biometric verification of the user **440** as described below with reference to FIG. **6**. If the biometric verification of the user is successful, the key provides its code over the secure communications channel.

The code is utilized to authenticate the biometric key itself **450**, **460** as described below with reference to FIG. **7** and profile information is received. Responsive to successful authentication of the key, access is allowed **470** to the application. In the slot machine example, a new pop-up window can be spawned to indicate a successful age verification.

FIG. **5** is a flow chart illustrating a method **500** for enrolling biometric data of the user with the biometric key according to one embodiment of the present invention. An agent checks **510** an identification of the user and establishes a profile. The agent can be, for example, a government official, a notary, and/or an employee of a third party which operates the trusted key authority, or another form of witness. The agent can follow standardized procedures such as requiring identification based on a state issued driver license, or a federally issued passport in order to establish a true identity of the user.

The profile describes the user and can include, for example, the user's name, date of birth, age, passwords, account numbers, preferences etc. In some embodiments, the profile stores no or only limited information about the user. For example, the agent might store the date of birth of the user in the profile, but not store any other information about the user. In addition, the profile describes the biometric key and/or key authority. For the biometric key, the profile can store a value indicating the status of the key, such as whether the key is in-service, out-of-service, abandoned, lost, stolen etc. For the key authority, the profile can store a value identifying the key authority.

The agent also collects and persistently stores **520** biometric data from the user. To do so, a fingerprint or eye retina can be scanned and converted to data which is then persistently stored in the biometric key. In one embodiment, the agent does not retain the biometric data. Since this step occurs under control of the agent, the agent can be certain that the biometric data stored within the key matches the user who presented the identification. The agent also obtains the code (e.g., device ID) from the biometric key in which the biometric data was stored. The agent associates the code and the profile using a table and/or other data structure.

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**).

FIG. **7** is a flow chart illustrating a method **700** for authenticating a biometric key according to one embodiment of the present invention. The code is wirelessly received **710**. A request for authentication of the code is sent to the trusted key authority **720**. The trusted key authority determines whether the code is authentic **730** (i.e., it was created through an established enrollment process) and has a valid status (e.g., has not expired). 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 **740** (such as the user's age). If authentication is not successful, authentication fails **750** and the message to the application indicates that the user should be denied access.

In some embodiments, the biometric key provides multiple codes and/or other data values. For example, the key can provide a device ID code that the authentication module can provide to the trusted key authority in order to authenticate the key, and the key can provide a secret decryption value that can be used to communicate with the biometric key. As used herein, the term "code" is intended to include one or more of these values, depending upon the specific embodiment.

The order in which the steps of the methods of the present invention are performed is purely illustrative in nature. The steps can be performed in any order or in parallel, unless otherwise indicated by the present disclosure. 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. Software embodying the present invention may comprise computer instructions in any form (e.g., source code, object code, interpreted code, etc.) stored in any computer-readable storage medium (e.g., a ROM, a RAM, a magnetic media, a compact disc, a DVD, etc.). Such software may also be in

the form of an electrical data signal embodied in a carrier wave propagating on a conductive medium or in the form of light pulses that propagate through an optical fiber.

While particular embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that changes and modifications may be made without departing from this invention in its broader aspect and, therefore, the appended claims are to encompass within their scope all such changes and modifications, as fall within the true spirit of this invention.

In the above description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the invention. It will be apparent, however, to one skilled in the art that the invention can be practiced without these specific details. In other instances, structures and devices are shown in block diagram form in order to avoid obscuring the invention.

Reference in the specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment.

Some portions of the detailed description are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to an apparatus for performing the operations herein. This apparatus can be specially constructed for the required purposes, or it can comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program can be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and modules presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems can be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatuses to perform the method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages can be used to implement the teachings of the invention as described herein. Furthermore, 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. Of course, wherever a component of the present invention is implemented as software, the component can be implemented as a standalone program, as part of a larger program, as a plurality of separate programs, as a statically or dynamically linked library, as a kernel loadable module, as a device driver, and/or in every and any other way known now or in the future to those of skill in the art of computer programming. Additionally, the present invention is in no way limited to implementation in any specific operating system or environment.

It will be understood by those skilled in the relevant art that the above-described implementations are merely exemplary, and many changes can be made without departing from the true spirit and scope of the present invention. Therefore, it is intended by the appended claims to cover all such changes and modifications that come within the true spirit and scope of this invention.

What is claimed is:

1. A method comprising:

receiving, at a smartphone, an identification (ID) code from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones;

persistently storing biometric data and the ID code on the smartphone, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan of a legitimate user;

receiving, at the smartphone, scan data from a biometric scan using the smartphone;

comparing, using the smartphone, the scan data to the biometric data;

determining whether the scan data matches the biometric data; and

responsive to a determination that the scan data matches the biometric data, wirelessly sending, from the smartphone, the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority, a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

2. The method of claim **1**, further comprising:

Receiving a request for biometric verification, and responsive to a determination that the scan data does not match the biometric data, indicating the smartphone

cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.

3. The method of claim **1**, wherein completing the transaction includes accessing an application.

4. The method of claim **1**, wherein the transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code includes the third-party trusted authority sending an indication that the third-party trusted authority authenticated the ID code to another party.

5. A smartphone comprising:

a persistent storage having an input that receives an identification (ID) code from a third-party trusted authority, and biometric data, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan, of a legitimate user, the ID code uniquely identifying the smartphone among a plurality of smartphones, the persistent storage storing the biometric data and the ID code, the persistent storage having an output configured to provide a first set of biometric data and the ID code for use on the smartphone;

a validation module, coupled to communicate with the persistent storage to receive the biometric data from the persistent storage, the validation module having a scan pad to capture scan data from a biometric scan, the validation module comparing the scan data to the biometric data to determine whether the scan data matches the biometric data; and

a wireless transceiver that, responsive to a determination that the scan data matches the biometric data, sends the ID code for comparison by the third-party trusted authority against one or more previously registered ID codes maintained by the third-party trusted authority, a transaction being completed responsive to the third-party trusted authority successfully authenticating the ID code, wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account.

6. The smartphone of claim **5**, wherein the ID code is transmitted to the third-party trusted authority over a network.

7. A system, comprising:

a smartphone that persistently stores biometric data and an ID code, wherein the biometric data is one selected from a group consisting of facial recognition, a fingerprint scan, and a retinal scan data of a legitimate user, and the ID code is received from a third-party trusted authority, the ID code uniquely identifying the smartphone among a plurality of smartphones, the smartphone configured to indicate that a biometric authentication is requested, the smartphone configured to wirelessly send the ID code to the third-party trusted authority for authentication responsive to determining that scan data from a biometric scan performed using the smartphone matches the biometric data of the legitimate user, wherein a transaction is completed responsive to successful authentication of the ID code by the third-party trusted authority, wherein the transaction being completed includes accessing one or more from a group consisting of a casino machine, a keyless lock, an ATM machine, a web site, a file and a financial account; and

the third-party trusted authority operated by a third party, the third-party trusted authority storing a plurality of legitimate ID codes and authenticating the ID code received based on a comparison of the ID code received and the legitimate ID codes included in the plurality of the legitimate ID codes.

8. The system of claim **7**, wherein the smartphone receives an authentication request, and in response, requests biometric scan from a user to generate the scan data and, when the smartphone cannot verify the scan data as being from the legitimate user, the smartphone does not send the ID code.

9. The system of claim **7**, wherein completing the transaction includes accessing an application.

* * * * *

EXHIBIT 5

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 **JURY TRIAL REQUESTED**

DECLARATION OF CREED JONES, PHD IN SUPPORT OF

DEFENDANT'S OPENING CLAIM COSNTRUCTION BRIEF

I. INTRODUCTION

I, Creed Jones, declare as follows:

1. I have been asked by counsel for Apple Inc. ("Apple" or "Defendant") to analyze U.S. Patent No. 8,352,730 ("the '730 patent"). I understand that the party asserting the '730 patent in this matter is Proxense, LLC ("Proxense" or "Plaintiff").
2. I am familiar with the technology at issue in the period prior to the earliest priority date that is claimed by the '730 patent, which I understand is December 20, 2004. I have used December 20, 2004 as the "time of invention" for my analysis as the person of ordinary skill in the art. In formulating my opinions, I have relied upon my knowledge, education, training, skill, and experience in the relevant art, as well as on the documents and information described below. I have also considered the viewpoint of a person of ordinary skill in the art ("POSITA") as of the time of the invention.
3. In preparing this Declaration, I have reviewed the '730 patent and its file history, the constructions proposed by the parties, and any other documents referenced in this Declaration.
4. I have personal knowledge of all facts set forth herein. I expect to be available for deposition and to testify competently to the matters contained in this declaration if called upon to testify.
5. This report is based on information currently available to me. I may continue my investigation and study, which may include a review of documents and information that have not yet been produced, as well as deposition testimony from depositions for which transcripts are not yet available, may yet be taken in this proceeding or which I have not yet been provided. Therefore, I expressly reserve the right to expand or modify my opinions as my investigation and study continue, and to supplement my opinions in

response to any additional information that becomes available to me. Moreover, I reserve the right to provide rebuttal testimony regarding any analyses and opinions raised in opposition or rebuttal to my report.

6. I am being compensated for my work in this matter at the rate of $375 per hour. I am also being reimbursed for all costs I incur in connection with my work. My compensation in this matter is not contingent upon the rendering of any opinion or the outcome of the litigation. I have no financial interest in the outcome of this litigation.

7. This Declaration is a statement of my opinion on issues related to claim construction of the claims in the ’730 patent. I reserve the right to supplement my opinions expressed in this Declaration to address any new information obtained in the course of this proceeding, including any expert opinion provided by Proxense.

II. BACKGROUND & QUALIFICATIONS

8. I have a Ph.D. degree in Computer Engineering from Virginia Polytechnic Institute and State University (“Virginia Tech”). I also have a M.S. degree in Electrical and Computer Engineering and a B.S. degree in Electrical Engineering from Oakland University.

9. I am currently a Collegiate Professor in the Electrical and Computer Engineering department of the College of Engineering at Virginia Tech. Previously, I was a Professor of Computer Science at California Baptist University, and at Seattle Pacific University.

10. For more than 25 years, I have studied, designed, and worked in the field of image processing, biometric identification, computer science, and software development. My experience includes numerous years of teaching and research, with research interests including image processing, computer vision and machine learning.

11. I have been active in the field of image processing since 1983, and I have extensive experience in the development of image processing algorithms and software. I hold seven

US patents in image processing systems and methods. My areas of expertise have included multi-spectral and hyperspectral imagery, automated inspection, optical character recognition, image formation and capture, and biometric feature extraction and matching.

12. I have been a developer of image processing software for over 30 years. I have implemented image processing and machine learning solutions in C, C++, Java, Python, MATLAB and assembly programming languages, using a large number of platforms and environments including OpenCV, ImageJ, CImg, NIH Image, SAS, numpy, scikit, PyTorch, TensorFlow and several proprietary packages. I have also managed groups of image processing software developers in several organizations.

13. I am a co-founder and the Chief Technology Officer of Globe Biomedical, a medical device start-up company located in Riverside, CA. Globe was founded to commercialize patented technology that uses imaging to monitor the progress of eye diseases, including glaucoma. This technology was invented by me and a colleague at California Baptist University.

14. I received my Bachelor of Science degree in Electrical Engineering from Oakland University in 1980, my Master of Science degree in Computer and Electrical Engineering from Oakland University in 1982, and my Doctor of Philosophy degree in Computer Engineering from the Virginia Polytechnic Institute and State University in 2005. My doctoral research and dissertation was in the area of biometric identification. Specifically, my dissertation is titled "Color Face Recognition using Quaternionic Gabor Wavelets" and comprises the development of one of the first full-color face recognition algorithms and methods.

15. In biometrics, I have served as an algorithm developer, systems engineer, standards developer and independent consultant from 1998 to the present. While on the staff of

Sagem Morpho, I had responsibility for research and strategy in the areas of fingerprint capture systems and methods. Sagem Morpho has been the core technology supplier for many large-scale fingerprint identification systems in the law enforcement field, including the FBI Integrated Automated Fingerprint Identification System (IAFIS) and a number of state- and county-wide AFIS systems. I was a project engineer on a number of state AFIS system installations and upgrades. As such, I am familiar with both the core technologies of biometric identification as well as the systems-level engineering involved with the capture, encoding, storage, transmission and matching of biometric samples.

16. I have experience in several image-based biometric modalities: fingerprint, face, iris, vein pattern and hand geometry. My doctoral dissertation, *Color Face Recognition using Quaternionic Gabor Filters*, was the first description of a full-color face recognition algorithm using robust modern concepts and included both theoretical groundwork and a complete implementation in C++.

17. The ANSI-accredited body for the development of US National standards in Information Technology is INCITS, the International Committee for Information Technology Standards. From 2001 to 2006 I was the chair of the INCITS M1.3 subcommittee on standardization of biometric data interchange formats, as well as a key participant in its parent body, INCITS M1. During this time, I was also the technical editor of INCITS 378, Finger Minutia Format for Data Interchange, the most widely adopted standard for exchange of biometric feature data. I was also a key contributor to INCITS 381 - Fingerprint Image Data Format, INCITS 385 – Face Recognition Data Format, INCITS, and the BioAPI standard.

18. In the international arena, biometrics standards are developed under ISO/IEC Joint Technical Committee 1, Subcommittee 37. I was a frequent member of the US delegation to JTC1 SC37, and to its Working Group 3 on biometric data standards. I was the chief technical editor of ISO/IEC 19794, fingerprint minutiae data format, and contributed to many other international standards such as ISO/IEC 29794 – biometric sample quality.

19. I have been and am currently a member of several professional organizations and committees. I am a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the ANSI/INCITS M1 Committee for biometrics standards, chair of ANSI/INCITS M1.3 Task Group on Biometric Data Interchange Formats - chair (2001 – 2006), chair of ANSI/INCITS B10.9 Task Group on biometrics (2001), technical editor of ANSI/INCITS B10.8 biometric task force (1999 – 2001), and a member of the BioAPI Industry Consortium (1999 – 2001).

20. A copy of my curriculum vitae, which describes in further detail my qualifications, responsibilities, employment history, honors, awards, professional associations, invited presentations, and publications is attached to this declaration as **Appendix A**.

III. LEGAL PRINCIPLES

21. My opinions are informed by my understanding of the relevant law, which I have been provided by counsel.

22. I have been informed and understand that claims are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art ("POSITA") at the time of the alleged invention, in light of the patent specification and prosecution history. Such an individual is considered to possess ordinary skills and knowledge in a particular technical field, and is not an automaton.

23. I have also been advised that a POSITA is a hypothetical person who is capable of understanding the scientific and engineering principles applicable to the relevant art of the claimed subject matter. I understand that a POSITA is presumed to have known the relevant prior art at the time of the alleged invention.

24. I understand that the words in a claim are construed based on the "intrinsic evidence," which includes the claim language, language in other claims of the patent in question or other patents in the same family, the specification, and the prosecution including prior art cited in the prosecution history. I understand that it is also sometimes permissible to refer to "extrinsic" evidence, which is all information that is not "intrinsic evidence" and includes, among other things, dictionaries, technical treatises, prior art, and expert testimony. I understand that extrinsic evidence may be used to provide additional background for how a person of ordinary skill in the art would understand the claim terms. However, these extrinsic sources of evidence are inherently less reliable than the intrinsic evidence identified above.

25. Although the words in the claims are generally given their ordinary and customary meaning, I have also been informed that a patentee may choose to act as a lexicographer, coin new terms, or redefine a well-known term of art. I understand that when a patentee explicitly defines a claim term in the patent specification, then the patentee's definition control.

26. I have further been informed of "means-plus function" claim terms. I understand that means-plus-function claiming allows a patentee to claim functionality of an apparatus without reciting a specific structure within the claim itself. Instead, a means-plus-function claim relies on a corresponding structure found in the corresponding patent specification.

27. I understand that construing a claim term as a "mean-plus-function" term involves two analyses. I understand that the first analysis involves determining whether the term is drafted in "means-plus-function" format. I have been informed that a claim term that does not recite "means" is presumptively not a means-plus function term. However, this presumption may be overcome if a POSITA would believe the claim term does not recite sufficiently definite structure or else recites a function without reciting sufficient structure for performing that function. I further understand that the presumption against means-plus-function treatment may be overcome if the claim limitation uses a generic placeholder (also referred to as a "nonce" word), which is simply a substitute for the term "means."
28. I understand that the second analysis involves identifying the function or functions recited in the claim for the "means-plus-function" term, and the corresponding structure disclosed in the patent specification for performing the claimed function(s).
29. I understand that structure disclosed in the specification qualifies as "corresponding structure" if the intrinsic evidence clearly links or associates that structure to the function(s) recited in the claim. I further understand that where the claim recites multiple functions for the "means-plus-function" term, the specification must disclose corresponding structure to perform all claimed functions.
30. I further understand that, even if the specification discloses corresponding structure, the disclosure must be of adequate corresponding structure to achieve the claimed function. I further understand that a means-plus function term is indefinite if a POSITA would be unable to recognize the structure in the specification and associate it with the corresponding function in the claim.

31. I have been informed that claim construction is a matter of law and that the final claim constructions for this proceeding will be determined by the Court.

IV. PERSON OF ORDINARY SKILL IN THE ART

32. Applying the legal principles set forth above, it is my opinion that a person of skill in the art with respect to the ’730 patent at the time of the alleged invention would have had at least a bachelor’s degree in computer or electrical engineering or an equivalent engineering discipline, and at least three years of experience in the field of biometrics, encryption and security, or the equivalent. Additional education could substitute for professional experience, and significant work experience could substitute for formal education.

V. THE ’730 PATENT

33. The ’730 patent generally relates to “computerized authentication” using biometric data. ’730 patent at 1:15–18. The patent generally discloses a distributed form of biometric authentication involving a biometric key that persistently stores biometric data in a tamper-resistant format, a scanner that collects biometric data from a user, and an integrated device that compares the scan against the biometric data and sends a code, for example to an application, to indicate that the user was successfully verified. ’730 patent at 1:59-67.

34. An exemplary embodiment of the biometric key is depicted in Figure 2:

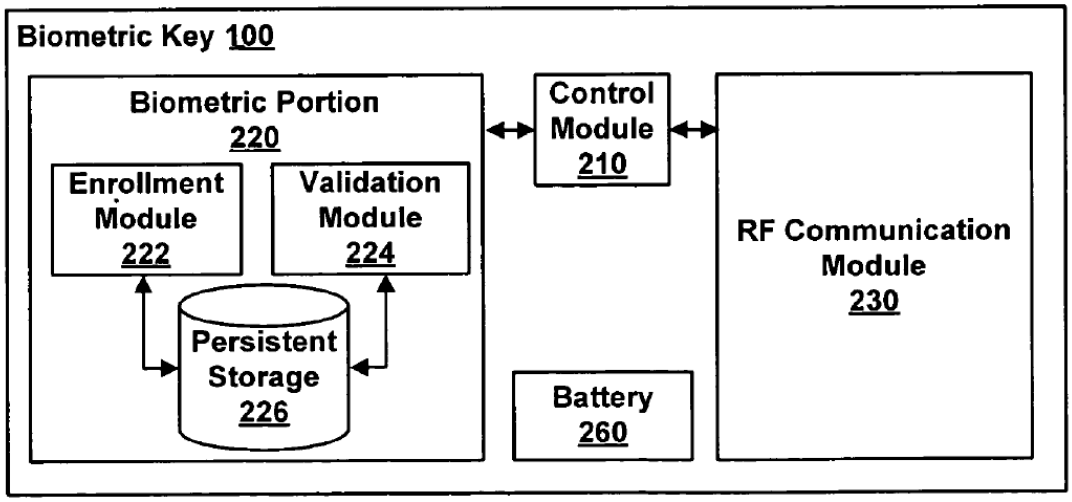


FIG. 2

'730 patent at Fig. 2.

35. Figure 2 depicts several elements pertinent to my analysis, including validation module 224, control module 210 and RF communication module 230, discussed in greater detail below.

36. I understand that Proxense contends that Apple infringes claims 1, 2, 5, 6, 8 and 9 of the '730 patent. The opinions set forth in this declaration relate to claim 8, which recites:

> 8. An integrated device for verifying a user during authentication of the integrated device, comprising:
>
> a memory stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the memory that is unable to be subsequently altered; wherein the biometric data is selected from a group consisting of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;
>
> 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 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, wherein the one or more codes and the other data values includes the device ID code; and

responsive to the agent authenticating the one or more codes and the other data values, a radio frequency communicator, receives an access message from the agent allowing the user access to an application, wherein the application is selected from a group consisting of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

'730 patent, claim 8.

VI. OPINIONS RELATING TO CLAIM CONSTRUCTION

37. I have been asked to provide my opinions relating to one claim term in claim 8 of the '730 patent, *i.e.* "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 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, wherein the one or more codes and the other data values includes the device ID code."

38. I understand that Apple and Proxense have offered the following constructions for this term:

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	No construction needed; plain and ordinary meaning beyond any terms that the Court previously construed in *Proxense v. Samsung.*

identifying legitimate integrated devices Structure: Indefinite.	

39. Applying the legal principles set forth above, it is my opinion that Apple's proposed construction for this term is correct.

A. The "verification unit…" term is a "means-plus-function" term.

40. The term "verification unit" is not a widely used term in the field, and does not have a well-understood structural meaning.

41. The word "unit" in the term "verification unit" is simply a generic placeholder, or "nonce word." It does not connote structure, much less sufficiently definite structure. In the context of this claim term, a POSITA would understand the word "unit" to simply be a synonym for "means."

42. The prefix "verification" also does not connote structure. Rather, a POSITA would understand the prefix "verification" to be purely functional language. It describes a function that is performed by the "unit," *i.e.* verifying. The specification does not define the general term "verification", but rather refers to several types of "verification" – biometric verification, user verification and age verification, for example. Claim 8 does not even specify which if any of the mentioned types of verification are of reference here, and no structure is described.

43. Nor does the entire phrase "verification unit" connote structure. The phrase "verification unit" is not a widely used term used in the field, and does not have a well-understand structural meaning. A POSITA would not understand the entire phrase "verification unit"

to connote any particular structure, but rather simply understand a "verification unit" to be something that verifies.

44. The phrase "verification unit" appears once in claim 8 of the '730 patent in the following limitation:

> 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 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, wherein the one or more codes and the other data values includes the device ID code; and

'730 patent, claim 8.

45. The surrounding claim language provides no indication as to what the structure of the claimed "verification unit" is.

46. Claim 8 first requires that "verification unit" be "in communication with the memory." However, this limitation does not indicate or suggest any particular structure for the claimed "verification unit." Rather, a POSITA would understand this limitation to simply require that the "verification unit" be able to communicate with the memory. While a "memory" is a well-known term connoting a class of structures, a POSITA would be aware of a wide range of structures capable of communicating with a memory, such as processors, cache controllers, direct memory access (DMA) units, error correcting code (ECC) devices and other structures. In a multi-level cache structure, even memory units themselves are "in communication" with other memory. Structures often described as "memory" include units such as network storage units and off-line archive products that would be communicated with via network connections that can be wired (Ethernet) or wireless (802.11 WiFi), so network transceivers and RF communication modules are often "in

communication with the memory". The requirement that the claimed "verification unit" be "in communication with the memory" does connote any particular structure for the claimed "verification unit."

47. Claim 8 next requires that the "verification unit" " receives scan data from a biometric scan for comparison against the biometric data." A POSITA would not understand this limitation to suggest or indicate any particular structure for the "verification unit." Rather this limitation is merely a function that is performed by the "verification unit."

48. Finally, claim 8 requires that "if the scan data matches the biometric data" then the "verification unit" "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, wherein the one or more codes and the other data values includes the device ID code." Again, this limitation simply describes a function performed by "verification unit," and does not suggest or indicate to a POSITA any particular structure for the "verification unit."

49. In short, the surrounding claim language describes what the "verification unit" does – not what structure the "verification unit" is.

50. The '730 patent specification also does not suggest or indicate the structure of the claimed "verification unit." The term does not even appear in the patent specification.

51. Because the term "verification unit" does not connote any particular structure, much less sufficiently definite structure to a POSITA, it is my opinion that the term "verification unit" is "means-plus-function" term.

B. The "verification unit…" term is indefinite, because the specification does not disclose sufficient corresponding structure for performing the claimed functions.

52. As set forth above, I understand that the construction of a "means-plus function" term requires identifying both the function(s) that the claim recites as being performed by the term and the corresponding structure which the specification clearly links to the recited function(s). Further, if the specification fails to disclose sufficient structure for performing each recited function, then the claim is indefinite.

53. Claim 8 of the '730 patent recites 2 functions performed by the "verification unit," *i.e.* (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."

54. The specification clearly links both claimed functions to elements depicted in Figure 2, reproduced below:

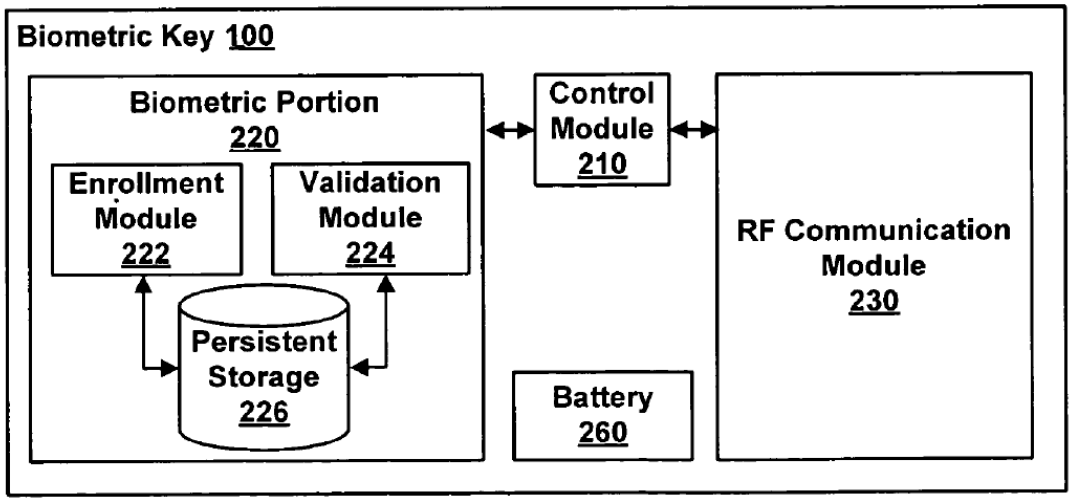


FIG. 2

'730 patent at Fig. 2.

55. The specification clearly links the first function ("receiv[ing] scan data from a biometric scan for comparison against the biometric data") to validation module 224. For example, the specification states:

> Validation module 224 can comprise scan pad 120 (FIG. 1) to capture scan data from a user's fingerprint (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module 224 determines whether the user's fingerprint matches the stored biometric data from enrollment.

Id. at 4:13-18.

56. From this passage, a POSITA would understand that the validation module "receives scan data from a biometric scan," *i.e.* the scan data from a user's fingerprint. A POSITA would further understand this scan data is "for comparison against the biometric data," *i.e.* the stored biometric data from enrollment.

57. A POSITA would not understand the described "validation module" to connote structure. Rather, just like the claim term "verification unit," the term "validation module" includes

purely functional language. The word "module" in the phrase "validation module" is simply a generic placeholder, or "nonce word." It does not connote structure, much less sufficiently definite structure. In the context of the phrase "validation module," a POSITA would understand the word "module" to simply be a synonym for "means." The prefix "validation" also does not connote structure. Rather, a POSITA would understand the prefix "validation" to describe a function that is performed by the "module," *i.e.* validating.

58. Nor does the entire phrase "validation module" connote structure. The phrase "validation module" is not a widely used term used in the field, much less a term with a well-understand structural meaning. A POSITA would not understand the entire phrase "validation module" to connote any particular structure, but rather simply understand a "validation module" to be something that validates.

59. However, the specification elsewhere describes specific structure for implementing validation module 224. Specifically, the specification states:

> Validation module 224 <u>can comprise scan pad 120 (FIG. 1) to capture scan data from a user's fingerprint</u> (e.g., a digital or analog representation of the fingerprint). Using the scan data, validation module 224 determines whether the user's fingerprint matches the stored biometric data from enrollment.

Id. at 4:13-18.

60. The specification further describes the structure of scan pad 120 as follows:

> Scan pad 120 can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner. Scan pad 120 can be sized to fit a thumb or other finger.

Id. at 3:28-30.

61. Thus, a POSITA would understand that the structure corresponding to the first recited function ("receives scan data from a biometric scan") is a "scan pad 120 (Fig. 1) [configured] to capture scan data from a user's fingerprint." *Id.* at 4:13-18. This scan pad

"can be, for example, an optical scanner using a charge coupled device, or a capacitive scanner." *Id.* at 3:28-30.

62. Turning to the second function of the "verification unit" (*i.e.*"if the scan data matches the biometric data, wirelessly send[ing] one or more codes…"), the specification describes this function as being performed by control module 210 and RF communication module 230 in Fig. 2 (reproduced above). For example, the specification states:

> Control module 210 coordinates between several functions of biometric key 100. In one embodiment, control module 210 provides a verification code upon successful verification of the user. More specifically, once biometric portion 220 indicates that a fingerprint scan matches biometric data that was collected during enrollment, control module 210 can trigger RF communication module 230 for sending a code indicating that the user was verified.

'730 patent at 3:55-62.

63. From this passage, a POSITA would understand that control module 210 provides a verification code upon successful verification of the user, *i.e.* "if the scan data matches the biometric data." A POSITA would further understand that control module 210 triggers RF communication module 230 for sending a code that the user was verified, *i.e.* wirelessly sending one or more codes." Thus, a POSITA would understand that the specification clearly links control module 210 and RF communication module 230 to the function "if the scan data matches the biometric data, wirelessly send[ing] one or more codes…"

64. Just as with the "validation module" depicted in Fig. 2, a POSITA would not understand control module 210 and RF communication module 230 to connote structure. Rather, "control module" and "RF communication module" include purely functional language. The word "module" is simply a generic placeholder, or "nonce word." It does not connote structure, much less sufficiently definite structure. In the context of the phrases "control module" and "RF communication module," a POSITA would understand the word

"module" to simply be a synonym for "means." The prefixes "control" and "RF communication" also do not connote structure. Rather, a POSITA would understand the these prefixes to describe a function that is performed by the "module," *i.e.* control or RF communication functions.

65. Nor do the entire phrases "control module" and "RF communication module" connote structure. Neither phrase is a widely used term used in the field, much less a term with a well-understand structural meaning. A POSITA would not understand the entire phrases "control module" and "RF communication module" to connote any particular structure, but rather simply understand these modules to be something that provides control or RF communication functions, respectively.

66. The specification elsewhere describes specific structure for implementing RF communication module 230. Specifically, the specification states:

> Radio frequency (RF) communication module 230 is, for example, a transceiver or other mechanism for wireless communication. RF communication module 230 can send and receive data (e.g., the code) as modulated electromagnetic signals. In one embodiment, RF communication 230 can be optimized for low-power usage by, for example, using short range transceivers. RF communication module 230 can actively send out connection requests, or passively detect connection requests.

'730 patent at 4:56-64.

67. However, the specification does not describe any structure for implementing control module 210. Instead, control module 210 is simply depicted as a black box in Figure 2 for performing various control functions without any description of a structure for performing these functions. In fact, the specification expressly states that control module 210 is not any particular structure, but rather "merely a grouping of control functions":

> Note that control module 210 of FIG. 2 is merely a grouping of control functions in a central architecture, and in other

> embodiments, the control functions can be distributed between several modules around biometric key 100.

Id. at 3:66-4:3. This passage further notes that control module 210 need not even be present, but rather the control functions "can be distributed" between other modules in the biometric key.

68. Thus, a POSITA would not understand the specification to disclose any structure for implementing control module 210.

69. Because the specification clearly links the second recited function for the claimed verification unit (*i.e.*"if the scan data matches the biometric data, wirelessly send[ing] one or more codes…") to control module 210 and RF communication module 230, but does not disclose any structure for control module 210, the specification fails to disclose sufficient structure for performing the recited function.

70. Applying the legal principles above, it is therefore my opinion that the "verification unit" term in claim 8 of the '730 patent is indefinite, because the patent specification fails to disclose sufficient structure for performing each recited function.

VII. CONCLUSION

71. I hereby declare under penalty of perjury, under the laws of the United States of America, that I believe that the foregoing statements, analysis, and opinions are true and correct.

Executed on November 4, 2024 in Christiansburg, VA.

Creed Jones

APPENDIX A

Creed F. Jones III, PhD

creed@creedjones.com / crjones4@vt.edu
206.852.3216 (mobile)

Experience

Collegiate Professor and Assistant Graduate Director for Master of Science programs, Virginia Polytechnic Institute and State University, Blacksburg, VA, current

- Full professor in the Bradley department of Electrical and Computer Engineering
- Research interests include machine learning, ophthalmic imaging and image processing
- Teaching professor of graduate and undergraduate courses

Principal, Creed Jones Associates LLC, Christiansburg, VA, current

- Independent consulting in machine learning and biometrics
- Research and development
- Expert witness services

Founder and Chief Technology Officer, Globe Biomedical LLC, Riverside, CA, current

- Development of image-based wearable medical device for monitoring of glaucoma
- Strategic leadership of corporate and R&D efforts

Associate Dean for Graduate Programs, and Tenured Professor of Engineering, California Baptist University, Riverside, CA, 2013-2019

- Full professor in the Computing, Software and Data Sciences department
- Research interests include ophthalmic imaging, biometrics, advanced analytics and image processing
- Developed and led the first five MS programs in the College of Engineering
- As a member of the Dean's cabinet, participate in the administration of the College of Engineering
- Teaching professor of graduate and undergraduate courses

Senior Research Scientist, Strategic Analytics, Humana Inc., Louisville, KY, 2006-2013

- Led a team of scientists and analysts performing machine learning and analytics in both clinical and business realms
- Research and development in data mining for consumer health insights
  - Developed an inferential model to impute BMI values to members from administrative claims data
  - Led development of a predictive model to identify members at risk of an Adverse Drug Event
- Developed and led Humana's Statistical Residency program for entry-level analysts

Associate Professor of Computer Science, Seattle Pacific University, Seattle, WA, 2003-2007

- Tenure-track teaching professor in the Department of Computer Science
- Major teaching interests were programming, image processing and networks

Independent Consultant, Creed Jones Associates LLC, 2003-2006

- Consulting in the areas of biometric algorithms and industrial image processing
- 18-month development of a new biometric algorithm; development of a data interchange format for a behavioral biometric; and creation of a recognition method for a novel industrial symbology

Senior Product Engineer, Sagem Morpho Inc (now MorphoTrak), Tacoma, WA, 1999-2007

- Biometric product / systems engineering, standards development lead and industry liaison
- Represented SMI on national and international biometrics standards development committees

Technical Director, Avéreon Research (now a division of Bally Gaming), Bellevue, WA, 1998-1999

- Co-founder and Technical Director
- Secured initial development contract, defined product line, led development efforts
- Avéreon was a start-up company providing image processing solutions to OEM customers

Director of Vision Systems Integration, Technical Director and **Director of Operations**, FSI Automation / Optimas Corporation, Bothell, WA, 1996-1999

- Created and led the vision systems development team; later led all technical activities

Lead Systems Engineer, Perceptics Corporation (a Northrop Grumman subsidiary), Knoxville, TN

- Systems and software engineering of image processing products – automated license plate reader, cargo container identification system, contact lens inspection system, food package inspection system

Primary Technical Competencies

- Image processing and computer vision
- Machine learning, predictive modeling, data mining and clustering
- Biometric identification, especially image-based modalities
- Software Development in Python, Java, MATLAB, C++, SAS and assembly language
- Problem definition, identification of key insights and communication to stakeholders

Education

Ph.D. in Computer Engineering, Virginia Polytechnic Institute and State University**,** Blacksburg, VA

- 2005; Dissertation: *Color Face Recognition using Quaternionic Gabor Wavelets*

M.S. in Computer and Electrical Engineering, Oakland University, Rochester, MI

- Concentrations: image processing and controls

B.S. in Electrical Engineering, Oakland University, Rochester, MI

Reviewed Publications

Articles and Conference Papers:

- Rickard, M., J. Park, C. Jones, A. Sit and P. Davey. "Development of a novel wearable intraocular pressure monitor based on image tracking of exposed sclera", 2020 ARVO Annual Meeting
- Rickard, M., J. Butler, C. Jones, J. Park, A. Hassel, J. Villegas, C. Van Zant, A. DeWolf, N. Kawaguchi, S. Truitt and N. Lazkani, "Development of a Nanofabricated Sensor for Monitoring Intraocular Pressure Via Ocular Tissue Strain", IEEE EMBC 2019, Berlin, DE, July 2019.
- Rickard, M., C. Jones, N. Lazkani, L. Macy, J. Park, J. Key, C. Gipson-Bean, J. Gentry, and M. Saenz, " Scleral strain measurements near the limbus using in vivo imaging", ARVO Imaging 2018, Honolulu, HI, April 2018.
- Rickard, M., C. Jones, C. Gipson-Bean, J. Park, E. Sutter, J. Jacobson, and J. LaMotte, "Geometric measurements of natural features at the temporal limbus in support of an image-based, real-time IOP sensing system", Academy 2016 Anaheim, American Academy of Optometry, November 2016.
- Rickard, M., C. Jones, C. Gipson-Bean, J. Park. "Image processing to measure scleral strain near the limbus using digital microscopy in porcine eyes", 2016 ARVO Imaging in the Eye conference, April 30, 2016, Seattle, WA.
- Rickard, M., C. Jones, J, Cox, J. DeVore, A. Castro, J. Brannen, "Scleral strain near the limbus using digital microscopy of natural features in porcine eyes", 2015 ARVO Annual Meeting, May 3-7, 2015, Denver, CO.
- Rickard, M., C. Jones, M. Migdal, N. Reyes, and A. Murguia, "Experimental Investigation of RFID Range for Intraocular Implants", Proc. 10th IASTED International Conference on Biomedical Engineering, June 2014, Zurich, Switzerland.
- Creed F Jones III and A. Lynn Abbott, "Color Face Recognition by Hypercomplex Gabor Analysis", Proc. IEEE Int'l Conf. on Automatic Face and Gesture Recognition, 2006. April 2006, pp. 126-131.
- Creed F Jones III and A. Lynn Abbott, "Optimization of Color Conversion for Face Recognition," *EURASIP Journal of Applied Signal Processing*, 2004:4, pp. 522-529.

- Scalera, J.E.; Jones, C.F., III; Soni, M., Bucciero, M.B., Athanas, P.M., Abbott, A.L., Mishra, A., "Reconfigurable Object Detection in FLIR Image Sequences," *Proc. 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, 2002. 22-24 April 2002, pp. 284-285.
- Jones, C.F., III; Christman, M., "Genetic Algorithm Solution of Vigenère Alphabetic Codes," *Proc. IEEE Mountain Workshop on Soft Computing Industrial Applications*, 25-27 June 2001, pp. 59-63.
- Creed F. Jones III and James C. Griner, "An Image Processing System to Inspect Foil-packaged Food," *Proc. Food Process Automation Conference III*, 9-12 February 1994, pp. 55-61.
- Creed Jones and John Merva, "Vision-Based Process Control of Circuit Film Emboss," *Proc. Vision West*, Society of Manufacturing Engineers, 1986 (received best paper award for conference)

Technical Standards:

- INCITS 378-2004, Finger Minutiae Format for Data Interchange; US national standard for exchange of fingerprint minutiae biometric data (technical editor)
- ISO/IEC 19794-2:2005, Biometric Data Interchange Formats — Part 2: Finger Minutiae Data; international data format standard for minutiae-based fingerprint representation (chief editor)
- ISO/IEC 19794-9, Biometric Data Interchange Formats – Part 9: Vascular Image Data; international data format standard for vein pattern data (co-editor)

Other Publications

Biometrics: Identifying the Issue (joint article), MOVE (the magazine of the American Association of Motor Vehicle Administrators), Winter 2000

Invited Presentations and Workshops

Imaging for Glaucoma Detection, International Conference on Innovation & Entrepreneurship, Kunshan, China, December 2016
Computer Science as a Career, Riverside STEM Academy symposium, April 2015
Consumer Obesity Modeling, Humana SAS day, October 2010
Using Predictive Modeling to Forecast Member Health and Wellness, National Predictive Modeling Summit, 2010
Human Identification Applications and Challenges, University of Washington, May 26, 2006
The INCITS 378 standard, 2006 CardTech/SecurTech Conference, May 4, 2006
Is Automated Face Recognition Better in Color? Biometric Seminar, Mitretek Systems, May 17, 2005
Point of Sale Biometrics, 2002 Biometric Consortium Conference, September 24, 2002
Paying at your Fingertip: Dawning of the Biometric Age, nacs.tech, April 23, 2002
Emerging Trends in Biometrics, Integrated Justice Information Systems Symposium, March 27, 2002
Developing a BioAPI compliant application, 2000 Biometric Consortium Conference, April 2000

Expert Witness Experience (partial list)

Expert report, deposition and testimony in CrossMatch vs. Suprema (US ITC) for Fenwick & West
Expert report and deposition in ImageWare vs. M2SYS/Neurotechnology for San Diego IP Law
Several IPR review reports of existing patents, for Unified Patents
Expert report and deposition in The Hillman Group, Inc. vs. KeyMe, LLC for Quinn Emanuel
Expert reports in Maxell vs. Apple for DLA Piper
Other engagements ongoing or confidential (including reports and depositions)

Affiliations and Memberships

Senior Member, Institute of Electrical and Electronic (2000 - present)
ANSI/INCITS M1 Committee for biometrics standards
ANSI/INCITS M1.3 Task Group on Biometric Data Interchange Formats - chair (2001 - 2006)
ANSI/INCITS B10.9 Task Group on biometrics – chair (2001)
ANSI/INCITS B10.8 biometric task force – technical editor (1999 - 2001)
BioAPI Industry Consortium – member / participant (1999 – 2001)

Courses Taught

Image Processing
Applications of Machine Learning
Computer Architecture for SW Engineers
Software Construction
Imaging and Sensing for Engineers
Computer Vision
Artificial Intelligence
Introductory Programming (in both Java and C++)
Introduction to Logic System Design
Software Project Management

Patents

In application (2023) – PCT Application WO2023205688A1 – "Automated Grading and Assessment of Coins"
In application (2021) – US Patent Application US2021/0275019 A1 –Systems and Methods for Monitoring Eye Health"
In application (2016) – PCT Application WO2016029032A1 – "Systems and Methods for Monitoring Eye Health"
Chinese Patent #107,072,528B – "System and Method for Monitoring Eye Health", July 2, 2021
US Patent #10,806,341 – "Systems and Methods for Monitoring Eye Health", October 20, 2020
US Patent #9,770,169 – "Systems and Methods for Monitoring Eye Health", September 26, 2017
US Patent #8,543,428 – "Computerized System and Method for Estimating Levels of Obesity in an Insured Population", September 24, 2013
US Patent #6,298,171 – "System for Reading Data Glyphs", October 2, 2001
US Patent #6,078,698 – "System for Reading Data Glyphs", June 20, 2000
US Patent #5,515,159 – "Package Seal Inspection System", May 7, 1996
US Patent #5,081,685 – "Improved Method and Apparatus for Reading a License Plate", January 14, 1992

Graduate Students Supervised

At Virginia Tech:

Deekshit Myakala, MEng 2024: Underwater Image Enhancement Using VGG-16 Architecture Model
Sasweth Rajanarayanan, MEng 2023: Design and Evaluation of One Shot Learning based approaches to Face Recognition
Cole Sims, MEng 2023: Predicting Win Probability Added and Tackle Force to Create a Decision Support Tool for NFL Coaches
Christopher Pham, MS 2023: Understanding Human Imagination Through Diffusion Models
Aakriti Saini, MEng 2023: Twitter Bot Detection using Machine Learning
Deniz Aytemiz, MEng 2023: Bimodal Deep Learning Architecture for Malware Classification
Ryan Yih-Yun Liu, MEng 2023: High Resolution Mixed Neural Style Transfer with Stable Diffusion Text-To-Image Prompt Generation
Adrian Ruvalcaba, MEng 2023: Precise Tumor Segmentation in Vestibular Schwannoma

Manthan Shah, MEng 2023: GPU-Systems Level Analysis of YOLOv7 Inference Performance and Identification of Optimization Opportunities
Craig Wormack, MS 2023: Improvement in Frame Prediction using Optical Flow
Prayati Dutta, MEng 2023: Prediction of Breast Cancer from Ultrasound Images
Braedon Dickerson, MEng 2023: Code Architecture Modeling with Augmented Reality
Aakriti Saini, MEng 2023: Twitter Bot Detection using Machine Learning
Kaushik Ganesan, MEng 2023: Misogynistic Meme Detection
Saksham Raina, MS 2022: Exploring Involution in Deep Convolutional Networks
Surasith Boonaneksap, MS 2021: The Study of Potential Benefits of Deep Convolutional Neural Networks for Segmenting Unruptured Intracranial Aneurysms from 3D MRA-TOF Images
Chieh Tsao, MEng 2021: An Increased-Accuracy Modified Random Forest Algorithm
Meghana Shakhapur, MEng 2021: Deep Anomaly Detection in Surveillance Videos
Niu Yuan, Meng 2021: Autonomous Robotic Mapping and Navigation using ROS and Gazebo
Yi Huang, MEng 2021: Cross-Domain Context-aware 3D Hand Pose Estimation
Shalini Ragothaman, MEng 2020: Machine Learning for Semantic Art Description
Yihao Hu, MEng 2020: Protein Secondary Structure Prediction with Cyclical Learning Rate and Jacobian Regularization
Nic Acton, MEng 2020: Interdisciplinary Technologist Program Design
Hitesh Baadkar, MEng 2021: Automated Rooftop Segmentation from Aerial Imagery

At California Baptist University:
Jonathan Key, MSSE 2016: A Mobile Application to Analyze Sclera Strain in Images of the Eye
Ronith Jukanti, MSSE 2017: Real-time Gesture Recognition on a Smartphone
Sunnykumar Kamani, MSSE 2017: An Enhanced Fingerprint Recognition Algorithm
Harshil S Parikh, MSSE 2017: Finger Vein Recognition System
Rishith Varala, MSSE 2017: Strategic Analysis in e-Commerce
Francis Lalwadi, MSSE 2018: Event Management System
Bhanu Manikonda, MSSE 2018: A Web Resource Tool for Tracking Human Resources
Riddhi Patel, MSSE 2019: Web-Enabled IoT System for Crop Planning

Awards

INCITS Team award as part of the M1 editorial team – 2006
INCITS Gene Milligan award for effective standards committee management – 2005
Gilbert Faison scholarship (Virginia Tech) – 2002
William A. Blackwell Award for best research presentation (Bradley departmental award) – 2001-2002
Exceptional Technical Achievement award – Perceptics Corporation – 1991
Oakland University School of Engineering Scholarship (four years)
Tau Beta Pi – Michigan Theta chapter

Academic and Professional Service

University Library Committee chair, Virginia Tech, 2019-2021
ECE Software and Machine Intelligence area chair, Virginia Tech, 2020-
Faculty Senate Representative, California Baptist University, 2014-2015
Instructional Development Committee, Seattle Pacific University (2004-2007, chair 2005-2007)
IEEE Student Branch Faculty Counselor, Seattle Pacific University (2005-2007)
Vendor co-chair, CCSC/NW 2005 conference

Reviewer, International Conference on Image Processing, 2006-2011
Reviewer, CCSC/NW 2006
Reviewer, *The Handbook of Computer Networks*, John Wiley, 2006
Reviewer, *ACM Computing Reviews,* 2007-current

Security clearances

US Department of Defense Secret (inactive), granted October 16, 1986
US Department of Justice Secret (inactive), granted 1986

Creed Jones, PhD

Expert Witness Activity, 2010-2024

Retained by Fenwick & West for the defendant in CrossMatch vs. Suprema in the USITC; U.S. Patent Nos. 5,900,993, 6,483,932, 7,203,344 and 7,277,562.
Wrote reports, was deposed and testified at the USITC
Case involved patents related to fingerprint capture and recognition, and image compression; included source code analysis
Jul. 2010 – Apr. 2011

Retained by San Diego IP Law for the plaintiff in ImageWare vs. M2SYS et al.
CASE NO. 13-CV-0309-DMS-JMA in the US District Court for the Southern District of California; U.S. Patent Nos. 7,298,873, 7,362,884, 7,596,246 and 7,606,396.
Wrote reports and was deposed
Case involved patents related to Image-based biometric verification software; included source code analysis
Mar. 2014 – Jun. 2014

Retained by Miles Stockbridge in IQS US Inc. vs. Prometric Inc.
Patent Trial and Appeal Board Case No. *unassigned*; U.S. Patent No. 7,773,779
Wrote expert declaration for inter-partes review
Case involved patents related to image-based biometric identification
Oct. 2016 – Jan. 2017

Retained by Erise IP Law in Unified Patents Inc. vs. SRR Patent Holdings LLC
Patent Trial and Appeal Board Case No. IPR2017-01514; U.S. Patent No. 8,799,088
Wrote expert declaration for inter-partes review
Case involved patents related to fingerprint recognition in an on-card scenario
Apr. 2017 – Jun. 2017

Retained by Oblon McClelland in Unified Patents Inc. vs. Pen-One Acquisition Group LLC
Patent Trial and Appeal Board Case No. IPR2017-*unassigned*; U.S. Patent Nos. 7.281,135 and 8,374,402
Wrote expert declaration for inter-partes review
Case involved patents related to dynamic signature verification systems
Jun. 2017 – Sep. 2017

Retained by Akin Gump in Unified Patents Inc. vs. Vindolor LLC
Patent Trial and Appeal Board Case No. IPR2019-00478; U.S. Patent No. 6,213,391
Wrote expert declaration for inter-partes review
Case involved patents related to biometric identification software
Nov. 2017 – Dec. 2017

Retained by Pierce Bainbridge in Hamilton vs. Speight
Civ. Action No. 2: 17-cv-0169-AB in the Eastern District of Pennsylvania
Wrote expert report
Case involved face recognition to verify use of an individual's identity without permission
Oct. 2018

Retained by Morgan Lewis related to video identification
In reference to a potential workplace injury compensation claim
Wrote expert report
Case involved face recognition to verify identity of an individual to a video image
Jun. 2019

Retained by Baker Donaldson for the defense in Horn vs. Marek
Civ. Action No. in the Circuit Court of Tennessee, Thirtieth Judicial District at Memphis
Wrote expert report
Case involves use of face recognition for confirming security camera identification
Mar. 2020 – Oct. 2021

Retained by DLA Piper for the defense in Maxell vs. Apple in the USITC
Wrote expert reports
Case involved several patents related to TouchID
Oct. 2020 – Mar. 2021

Retained by Quinn Emanuel for the defense in The Hillman Group, Inc. vs. KeyMe, LLC
No. 16-346C in the United States Court for the District of Delaware
Wrote export report and was deposed
Case involved image processing and machine learning for automated key cutting
Nov. 2020 – Jun. 2021

Retained by Williams Mullen for the plaintiff in Geospatial Technology Associates LLC vs. USA
No. 16-346C in the United States Court of Federal Claims
Wrote export reports and was deposed several times
Case involves hyperspectral imaging software and algorithms; includes source code analysis
Mar. 2020 – current (awaiting trial)

Retained by DLA Piper for the defense in Hazlitt et al v. Apple Inc.
work is underway
Case is related to the Illinois Biometric Information Privacy Act
Oct. 2021 – current

Retained by Greenberg Traurig for the defense in Joseph Duron et al v. UniFocus, L.P.
Work is underway
Case is related to the Illinois Biometric Information Privacy Act
Sept. 2022 – current

Retained by Haynes Boone for the plaintiff in Apple Inc. v. Carbyne Biometrics, LLC.
Writing expert declarations for inter-partes review
Patent involves securing financial transactions
Oct. 2023 – current

Retained by Fish and Richardson for the defense in Samsara Inc. v. Motive Technologies Inc. in the USITC
Work is underway
Case involves patents in the DashCam technology area
April 2024 – current

EXHIBIT 6

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090 US

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Pacific Time Zone of the United States on the local date shown below:

Dated: July 5, 2011 By: /Kanda Ishihara/
Kanda v. Ishihara, Reg. No. 56,607

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT E

Sir/Madam:

Responsive to the Office Action mailed on March 2, 2011, which sets a shortened statutory period for response that expires on June 2, 2011. A petition for a one-month extension of time is submitted herewith.

Please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data ~~for~~ of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value ~~code~~ in a tamper-~~resistant~~ proof format written to ~~in~~ a storage element on the integrated device ~~that is written once and is not~~ that is unable to be subsequently altered ~~subsequently, wherein the code uniquely identifies the integrated device~~;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values ~~code~~ for authentication ~~to~~by an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices; and

responsive to authentication of the code by the agent, receiving an access message from the agent~~, to allow~~ allowing the user access.

2. (Previously Presented) The method of claim 1, wherein the code is transmitted to the agent over a network.

3. (Original) The method of claim 1, further comprising:

registering an age verification for the user in association with the code.

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

receiving a request for the code without a request for biometric verification; and

responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data ~~for~~ of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value ~~code~~ in a tamper~~-resistant~~ proof format~~, the persistent storage being~~ written ~~once and~~ to the storage that is unable to be subsequently altered ~~being not altered subsequently, wherein the code uniquely identifies the integrated device~~;

a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values ~~code~~ for authentication ~~to~~ by an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices; and

a radio frequency communication module for receiving an access message from the agent ~~that enables~~ allowing the user access, responsive to the agent authenticating the code.

11. (Canceled).

12. (Previously Presented) The integrated device of claim 10, wherein the code is transmitted to the agent over a network.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value ~~code~~ associated with a biometrically verified user, the ~~code~~ device ID code being registered with an agent~~, wherein the agent~~ that is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the code by the agent and the authentication determining whether the code is legitimate;

receiving an access message from the agent; and

in response to a positive ~~the~~ access message~~ being positive~~, ~~providing~~ allowing the user access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:
registering a date of birth or age with the agent.

18. (Original) The method of claim 15, further comprising:
establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:
a biometric key to store biometric data ~~for~~ of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value ~~code~~ in a tamper ~~resistant~~ proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending-the plurality of codes and other data values ~~code, the code being associated with the verified user and uniquely identifying the biometric key~~; and
an authentication module to receive the plurality of codes and other data values ~~code~~ and send the plurality of codes and other data values ~~code~~ to agent for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority ~~including~~ possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication module receiving ~~from the agent~~ an access message from the agent ~~to an application to allow~~ allowing the user to access the application.

20. (Original) The system of claim 19, wherein the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated March 2, 2011 (herein, "OA"). Claims 1, 10, 15, and 19 are amended herein. No new matter is added in view of the amendments to claims 1, 10, 15, and 19. Claims 1-3, 5, 7-10, 12-15 and 17-25 are pending upon entry of this amendment.

Response to Claim Objections

Claims 1, 10, 15, and 19 were objected to because of the following informalities: Claims 1, 10, 15, and 19 recite "... a third-party trusted authority including a list of codes identifying legitimate integrated devices." The Examiner has suggested that the claims be corrected to recite "... a third-party trusted authority that possess or has a list of codes identifying legitimate integrated devices." Applicants have amended claims 1, 10, 15, and 19 to correct the informalities. The Examiner is asked to withdraw the objection to claims 1, 10, 15, and 19.

Response to Rejections Under 35 U.S.C. § 103

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), and in view of Stanko (US 2005/0074126-hereinafter Stanko). This rejection is overcome in view of the amended claims.

As amended, independent claim 1 recites in part:

> persistently storing biometric data of the user <u>and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value</u> in a tamper-proof format written to a storage element on the integrated device <u>that is unable to be subsequently altered</u>;
>
> responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of the device ID codes uniquely identifying legitimate integrated devices; and

responsive to authentication of the code by the agent, receiving an access message from the agent allowing the user access.

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, the plurality of codes, which comprises a device ID code uniquely identifying the integrated device and a secret decryption value, is wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0007], [0009], [0031], and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal

identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper-proof format written to a storage element on the integrated device that is unable to be subsequently altered."

Hsu merely discloses a fob storing reference biometric data, which may be subsequently altered, and a private encryption key. Hsu col. 1, line 66-col. 2, line 4; col. 2, lines 37-38; col. 2, lines 63-64; col 5, lines 19-21. Hsu stores a reference image upon enrollment that may be altered after enrollment. Hsu col. 5, lines 19-21. However, the claimed invention stores biometric data of the user and a plurality of codes and other data values in a storage element that is unable to be subsequently altered. As Hsu discloses a method allowing subsequent alteration of stored biometric data, Hsu does not disclose "persistently storing biometric data of the user and a plurality of codes and other data values . . . written to a storage element on the integrated device that is unable to be subsequently altered," as claimed.

Column 5, lines 19-29 of Hsu are cited in the OA and disclose:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For additional security and convenience, the user may be asked to enroll two fingerprints, to allow for continued access if the user injures a finger, for example. In a verification mode of operation, the pre-processed fingerprint image is input to the correlator **28**, as indicated by line **43**, where it is compared with the reference image obtained from storage **32** over line **44**. The correlator **28** uses an appropriate technique to

Hence, column 5, lines 19-29 of Hsu discloses storing biometric data during enrollment which "is normally not repeated unless the fob is lost or damaged," but it can be repeated thereby altering the stored biometric data. This is patentably distinct from "storing biometric data of the user and a plurality of codes and other data values . . . written to a storage element on the integrated device that is unable to be subsequently altered," as claimed.

Additionally, Hsu does not disclose or suggest at least an integrated device "storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value" or "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication," as claimed.

Hsu merely discloses storing a single private key in addition to the biometric data on a fob. Hsu col. 1, lines 66- col. 2, line 4; col. 2 lines 37-38; and col. 2, lines 63-64. As Hsu discloses storing a single private key in addition to biometric data, Hsu does not disclose or suggest storing biometric data and a "plurality of codes and other data values." Furthermore, Hsu does not disclose or suggest "sending the plurality of codes and other data values for authentication," as claimed. Hsu discloses transmitting a cyclic redundancy code (CRC) from a portable device to a door. Hsu, col. 7 lines 17-34. The transmitted CRC, however, identifies a reference fingerprint image not the fob and is generated by the fob rather than stored in the fob.

Hsu, Abstract. Therefore, the CRC is not a code or other data value, as claimed, because it is not stored on the integrated device and is neither a device ID uniquely identifying the device nor a secret decryption value. Hsu discloses a fob with a private key which is neither a device ID nor sent for authentication. Additionally, Hsu does not disclose or suggest that the private key is unique, nor is a private key necessarily unique. Hsu also discloses that the private key is used for encrypting the CRC and not uniquely identifying the fob. Therefore, the private key is not a code or other data value, as claimed, because the private key at least is not sent for authentication, is not necessarily unique, and is not a device ID. As Hsu does not disclose even a single code or other data value, which is stored on an integrated device and sent for authentication as claimed, Hsu fails to disclose or suggest "a plurality of codes and other data values comprising a device ID uniquely identifying an integrated device and a secret decryption value." Therefore, Hsu fails to disclose at least "storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value" or "sending the plurality of codes and other data values for authentication," as claimed.

Stanko fails to remedy the deficient disclosure of Hsu. Rather, Stanko discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. However, Stanko merely redirects a ticket digitally signed using an authentication server's private key to a secure server that verifies the digital signature to allow access to the secure server. Stanko, ¶ [0055]. Stanko uses authentication of user credentials by one secure server to allow an authenticated user to access additional secure servers without retransmitting the user credentials. Stanko, ¶¶ [0048]-[0050]. Thus, Stanko uses a single set of user credentials for authentication and does not then transmit a plurality of codes and other data

values comprising a device ID code uniquely identifying an integrated device and a secret decryption value to a third-party trusted authority including a list of device ID codes identifying legitimate integrated devices responsive to scan data matching stored biometric data on the integrated device. Hence, Stanko also fails to disclose or suggest "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication by an agent that is a third-party trusted authority possessing a list of the device ID codes uniquely identifying legitimate integrated devices," as claimed.

In addition to failing to disclose or suggest multiple levels of authentication, Stanko fails to disclose or suggest either an integrated device storing a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value or sending the plurality of codes and other data values for authentication. Stanko merely discloses credentials including passwords, challenge-response, digital certificates, tokens, smart cards, or biometrics, or any combination thereof. Stanko ¶ [0047]. These credentials do not disclose a device ID or a secret encryption value. Therefore, Stanko does not disclose or suggest "storing biometric data of the user and a plurality of codes and other data values comprising a device ID code for uniquely identifying the integrated device and a secret decryption value."As Stanko does not disclose an integrated device storing codes and other data values, Stanko does not disclose the integrated device, "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication," as claimed.

Accordingly, the cited references, both alone and in combination, fail to disclose at least the claimed elements of "storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret

decryption value" or "responsive to a determination that the scan data matches the biometric data, wirelessly sending the plurality of codes and other data values for authentication." Thus, claim 1 is patentably distinct from the cited references, and reconsideration and withdrawal of its rejection is respectfully requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2, 5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23 depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 17, 18 and 23. Also, claims 20 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20 and 25. Hence, claims 12, 18, 20 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13, 14 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hsu and Stanko further in view of U.S. Patent Publication No. 2004/0129787 A1 to Saito et al. ("Saito"). This rejection is overcome in view of the amended claims.

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

Saito fails to remedy the deficient disclosure of Hsu. Rather, Saito discloses a smartcard system for biometric identification using ISO SmartCards. Saito, Abstract. Saito at least fails to at least disclose or suggest storing a plurality of codes and other data values comprising a device ID code uniquely identifying the ISO SmartCard and a secret decryption value in addition to biometric data on an ISO SmartCard. As Saito fails to disclose at least that the ISO SmartCard stores a plurality of codes and other data values, as claimed, it also does not disclose or suggest sending the plurality of codes for authentication. Like Hsu, Saito merely matches captured biometric data against multiple sources and does not also authenticate an integrated device by transmitting a device ID code uniquely identifying the integrated device to "an agent that is a third-party trusted authority possessing a list of device ID codes identifying legitimate integrated devices," as claimed. Saito merely verifies that captured biometric data matches locally stored data and, if the captured biometric data matches locally stored data, verifies that the captured biometric data matches data in a remote authentication system. Saito, ¶ [0008]. While Saito provides that the local match and remote match of the captured biometric data may be different, <u>only</u> biometric data is matched using the different systems. Saito, ¶ [0008]. There is no disclosure or suggestion in Saito of a device ID code uniquely identifying the integrated device or of a trusted-third party authority including a list of device ID codes identifying legitimate integrated devices. Hence, Saito also fails to disclose "responsive to a determination that the

scan data matches the biometric data, wirelessly sending the plurality of codes for authentication to an agent that is a third-party trusted authority possessing a list of device ID codes identifying legitimate integrated devices," as claimed.

Thus, claims 3, 13, 14 and 17 are patentably distinct from the cited references, both alone and in combination, and reconsideration and withdrawal of their rejection is respectfully requested.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: July 5, 2011 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9835
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

EXHIBIT 7

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090 US

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Pacific Time Zone of the United States on the local date shown below:

Dated: December 5, 2011 By: /Kanda Ishihara/
Kanda V. Ishihara, Reg. No. 56,607

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT F

Sir/Madam:

Responsive to the Office Action mailed on October 5, 2011, which sets a shortened statutory period for response that expires on January 5, 2012, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality of codes and 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, wherein the one or more codes and other data values includes the device ID code; and

responsive to authentication of the one or more codes and other data values [[code]]by the agent, receiving an access message from the agent allowing the user access to an application.

2. (Currently Amended) The method of claim 1, wherein the one or more codes and other data values are ~~code is~~ transmitted to the agent over a network.

3. (Currently Amended) The method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

4. (Canceled).

5. (Currently Amended) The method of claim 1, wherein the one or more codes and other data values indicate ~~code indicates~~ that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Currently Amended) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values [[code]]for authentication.

9. (Currently Amended) The method of claim 1, further comprising:

receiving a request for the one or more codes and other data values [[code]]without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values [[code]]without a request for biometric verification, sending the one or more codes and other data values [[code]]without requesting the scan data.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the storage that is unable to be subsequently altered;

a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality of codes and 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, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module for receiving an access message from the agent allowing the user access to an application, responsive to the agent authenticating the one or more codes and other data values[[code]].

11. (Canceled).

12. (Currently Amended) The integrated device of claim 10, wherein the one or more codes and other data values are ~~code is~~ transmitted to the agent over a network.

13. (Currently Amended) The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the ~~comprising a~~ device ID code uniquely identifying the integrated device and a secret decryption value associated with a biometrically verified, the device ID code being registered with an agent that is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices;

requesting authentication of the one or more codes and other data values [[code]] by the agent, wherein the authentication determines ~~and the authentication determining~~ whether the one or more codes and other data values are ~~code is~~ legitimate;

receiving an access message from the agent; and

in response to a positive access message, allowing the user access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:

registering a date of birth or age with the agent.

18. (Currently Amended) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the one or more codes and other data values [[code]]associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:

a biometric key to store biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the biometric key and a secret decryption value in a tamper proof format written to a storage element on the biometric key that is unable to be subsequently altered, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values includes the device ID code; and

an authentication module to receive the plurality of codes and other data values and send the plurality of codes and other data values to agent for authentication to determine whether the one or more codes and other data values are ~~code is~~ legitimate, wherein the agent is a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices, and responsive to the device ID code being authenticated, the authentication module receiving an access message from the agent allowing the user to access the application.

20. (Original) The system of claim 19, wherein the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data.

21. (Currently Amended) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the one or more codes and other data values[[code]].

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated October 5, 2011 (herein, "OA"). Claims 1-3, 5, 8-10, 12, 13,15, 18, 19 and 21 are amended. Claims 1-3, 5, 7-10, 12-15 and 17-25 are pending upon entry of this amendment.

Response to Claim Objections

Claim 15 is objected to because of the following informality: Claim 15 recites requesting authentication of the code by the agent and the authentication determining whether the code is legitimate." The Examiner, on page 4 of the OA, suggests that claim 15 recite ". . . requesting authentication of the code by the agent and determining whether the code is legitimate." Applicants have amended claim 15 to correct the informalities. Claim 15 now recites, in part, "requesting authentication of the one or more codes and other data values by the agent, wherein the authentication determines whether the one or more codes and other data values are legitimate." The Examiner is, therefore, asked to withdraw the objection to claim 15.

Response to Rejections Under 35 U.S.C. § 112, Second Paragraph

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-3, 5, 7-9, 10, 12-14, 15, and 17-19 are all rejected for reciting "the code" or depending on a claim that recites "the code" when it is unclear which one of the plurality of codes is being referred to. Independent claims 1, 10, 15 and 19 have been amended such that

"one or more codes and data values from the plurality of codes and other data values" are sent for authentication, "wherein the one or more codes and other data values includes the device ID code." All instances of "the code" in the claims have been amended to be either recite the "one or more codes and other data values" or the "device ID code." The Examiner is, therefore, asked to withdraw the 112, second paragraph, rejections of claims 1-3, 5, 7-9, 10, 12-14, 15, and 17-19.

Response to Rejections Under 35 U.S.C. § 103

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu et al. (US 6,041,410 A1, hereinafter Hsu), Stanko (US 2005/0074126-hereinafter Stanko) and in view of Beenau et al. (US 2004/0230488 A 1-hereinafter Beenau).

As amended, independent claim 1 recites in part:

> persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;
> responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan; . . .
> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality . . . wherein the one or more codes and other data values includes the device ID code; and
> responsive to authentication of the one or more codes and other data values by the agent, receiving an access message from the agent allowing the user access to an application.

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated

device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, one or more of the plurality of codes and other data values, including a device ID code uniquely identifying the integrated device are wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0007], [0009], [0031], and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on one or more of the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the one or more of the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." The Examiner argues, on pages 2-4 of the OA,

argues that Hsu teaches "persistently storing . . . in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." Specifically, the Examiner argues, on page 2 of the OA, that "tamper proof format" is disclosed:

> In response, Examiner respectfully disagrees. As disclosed, the fob in Hsu is a device that is highly resistant to reverse engineering, cloning and other techniques for tampering (*column 7, lines 63-65*). Therefore, information stored on the fob is tamper-proof, thus cannot be altered. The fob in Hsu stores at least private key of fob and

Respectfully, the Examiner is incorrect. "Highly resistant to . . . tampering" is not the same as "tamper proof" as "proof" by general definition indicates a greater degree of imperviousness than "resistant." Moreover, even assuming a common definition of "highly resistant to tampering" and "tamper proof," Hsu does not suggest or disclose, among other things, that what makes its device highly resistant to tampering is the format in which the information is stored on the device. For example, the high resistance to tampering may merely refer to the fact that the communications to/from the device of Hsu are encrypted thereby making it difficult to clone communications or reverse engineer the contents of the communication. Because Hsu fails to disclose or suggest that the format of the data stored on its device contributes to the device's high resistance to tampering, Hsu fails to disclose or suggest "persistently storing . . . in a tamper proof format" as recited by claim 1.

Neither Stanko nor Beenau remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose storing biometric

information in a tamper proof format. Beenau discloses storing biometric information on the database of a fob, but does not disclose that the biometric information is stored in a tamper proof format. At paragraph [0145] and [0161], Beenau discloses that biometric information can be stored in a secure database 212. At paragraph [0062], Beenau discloses that database 214 may be the same configuration as database 212 and that account data and/or unique fob identification code may be encrypted prior to storage on database 214. However, the fact that database 214 may be similar to database 212 does not mean that database 212 can be similar to database 214 and encrypt prior to storage. Additionally, there is no disclosure or suggestion that biometric information is or can be encrypted prior to storage. Moreover, there is no disclosure or mention that the biometric information is tamper proof in that new biometric information cannot be written or that existing biometric information cannot be modified. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

The Examiner argues on pages 3-4 of the OA:

> In response, Examiner respectfully submits that contrasting to Applicant's argument, column 5, lines 19-29 of Hsu does not disclose the biometric data stored in fob can be altered. On the contrary, column 5 lines 19-29 discloses when a fob is lost or damaged, the enrollment process can be repeated, which means additional fingerprints can be added and enrolled onto a different fob (because the old fob has been lost or damaged, that is, not working anymore). As such, it does not make sense if the enrollment is repeated on a lost or not-working fob. Therefore, Applicant's argument is not persuasive.

Respectfully, the Examiner is incorrect and mischaracterizes the disclosure of Hsu. Column 5, lines19-21 disclose:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For

Hence, Hsu discloses that biometric is **normally** not repeated unless the fob is lost or damaged. Hsu does not disclose or suggest, among other things, that enrollment is **unable** to be repeated absent the loss of or damage to the fob. Hsu discloses a common practice and not a feature/limitation of the technology. For example, the enrollment of Hsu may not **normally** be repeated unless the fob is lost or damaged because an individual's fingerprints remain relatively unchanged for long periods of time eliminating the desire to re-enroll and not because the person is unable to re-enroll biometric information. 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.

Neither Stanko nor Beenau remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose biometric information written to a storage element on the integrated device that is "unable to be subsequently altered." Beenau discloses storing biometric information on the database of a fob, but does not disclose that the database is written to a storage element on the fob that is unable to be subsequently altered. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Applicant's claim 1 is patentable over the cited references for additional reasons. Applicant's invention biometrically verifies the user at the integrated device prior to using a third-party trusted authority to authenticate the integrated device (based on one or more codes and other data values including the device ID code), and, responsive to authentication of the integrated device, allows the user access to an application. The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device.

By contrast, Hsu biometrically verifies the user at the integrated device before generating and encrypting a CRC based on the biometric information. The CRC is used for authentication at a door, which is not a third-party trusted authority, but is more similar to Applicant's "application." In other words, Hsu does not provide two level authentication because Hsu verifies biometric information only (encryption does not verify the integrated device itself) and access is allowed/disallowed by the "door" without using a third-party trusted authority. Applicant's integrated device verifies both biometric data and the integrated device itself, and requires authentication by a third-party trusted authority.

Stanko does not disclose or suggest verifying biometric data and at an integrated device prior to verifying the integrated device. Stanko discloses that an authentication server receives credentials, which may include biometrics, and the authentication server verifies the received credentials. Stanko, therefore, does not disclose verifying an integrated device itself nor does

Stanko disclose verifying biometric information at the integrated device prior to authenticating the integrated device itself at a third-party trusted authority.

Beenau, at paragraph [0081], discloses that a fob's unique identification code is sent to the reader, which authenticates the fob's unique identification code. By contrast, Applicant's invention relies on a third-party trusted authority to verify the device ID. Moreover, Beenau discloses that the fob's unique identification code is sent responsive to an interrogation signal and without prior biometric verification of the user. By contrast, Applicant's invention transmits the device ID code after successful biometric verification. The fob's unique identification code is verified, thereby allowing a user the ability to conduct transactions. Paragraph [0141] discloses that biometric information is used only as a secondary verification to complete transactions. By contrast, Applicant's invention uses the biometric verification as the primary, i.e., the first in time, verification. In paragraph [0141] requiring biometric secondary authentication, access has already been obtained (i.e., to obtain the spending limit) the biometric secondary authentication merely allows the execution of a transaction. By contrast, Applicant's invention requires biometric verification and device verification to precede access.

The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device as recited by claim 1. Therefore, claim one is patentably distinct from the cited references and allowance of claim 1 is requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2,

5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23 depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 18 and 23. Also, claims 20, 21 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20, 21 and 25. Hence, claims 12, 18, 20, 21 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13-14, and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hsu, Beenau, Stanko, and further in view of Saito et al. (US 2004/0129787 A1, hereinafter Saito).

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with the Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: December 5, 2011 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicant
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9835
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

EXHIBIT 8

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	13/710,109
FILING DATE:	December 10, 2012
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO:	10001-03653 US
CONFIRMATION NO:	5712

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: September 13, 2013 By: /Matthew Holmes/
Matthew Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT A

Sir/Madam:

Responsive to the Office Action mailed on June 13, 2013, which sets a shortened statutory period for response that expires on September 13, 2013, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method comprising:

persistently storing biometric data of [[the]]a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and [[the]]other data values for authentication by an agent that is a third-party trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

2. (Currently Amended) The method of claim 1, wherein the one or more codes and [[the]] other data values are transmitted to the agent over a network.

3. (Original) The method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

4. (Currently Amended) The method of claim 1, wherein the one or more codes and [[the]]other data values indicate that the biometric verification was successful.

5. (Original) The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Original) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Original) The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. (Original) The method of claim 1, wherein the application includes a file including medical information.

9. (Original) The method of claim 1, wherein the application includes a financial account.

10. (Currently Amended) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and [[the]]other data values for authentication.

11. (Currently Amended) The method of claim 1, further comprising:

receiving a request for the one or more codes and [[the]]other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and [[the]]other data values without a request for biometric verification, sending the one or more codes and [[the]]other data values without requesting the scan data.

12. (Currently Amended) An integrated device comprising:

a persistent storage [[to]]that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage and unable to be subsequently altered;

a verification module, coupled to communicate with the persistent storage, [[to]]that receives scan data from a biometric scan for comparison against the biometric data, and [[to]]that sends one or more codes and other data values from the plurality of codes and other data values for authentication by an agent, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module ~~for receiving~~ that receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

13. (Currently Amended) The integrated device of claim 12, wherein the one or more codes and [[the]]other data values are transmitted to the agent over a network.

14. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

15. (Original) The integrated device of claim 12 comprising:

an LED to be activated for requesting the biometric scan.

16. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and [[the]]other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority;

requesting authentication of the one or more codes and [[the]]other data values by the agent;

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values; and

in response to receiving the access message, allowing the biometrically verified user access to an application.

17. (Original) The method of claim 16, further comprising:

registering a date of birth or age with the agent.

18. (Currently Amended) The method of claim 16, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and [[the]]other data values associated with the biometrically verified user is received from the integrated device.

19. (Original) The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (Original) The method of claim 16, wherein the application includes a file including medical information.

21. (Original) The method of claim 16, wherein the application includes a financial account.

22. (Currently Amended) A system, comprising:

an integrated device ~~for storing~~ that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element in the integrated device that is unable to be subsequently altered, and [[for]]that wirelessly ~~sending~~ sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and [[the]]other data values include the device ID code; and

an authentication unit ~~for receiving~~ that receives the one or more codes and [[the]]other data values and sends the one or more codes and [[the]]other data values to an agent for authentication, and ~~for receiving~~ that receives an access message from

the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

23. (Currently Amended) The system of claim 22, wherein the integrated device receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate [[the]]scan data.

24. (Currently Amended) The system of claim 22, wherein when the integrated device cannot verify [[the]]scan data as being from the user, [[it]]<u>the integrated device</u> does not send the one or more codes and [[the]]other data values.

25. (Original) The system of claim 22, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. (Original) The system of claim 22, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

27. (Original) The system of claim 22, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. (Original) The system of claim 22, wherein the application includes a file including medical information.

29. (Original) The system of claim 22, wherein the application includes a financial account.

REMARKS

Claims 1-29 were presented for examination. Claims 1-29 stand rejected in the Office Action dated June 13, 2013 (herein, "OA"). Claims 1, 2, 4, 10-13, 16, 18 and 22-24 amended. Claims 1-29 are pending upon entry of this amendment.

Summary of Office Action

1. Claims 15 and 16 are objected to for alleged informalities.

2. Claims 1-5, 7, 10-18, 22-24 and 26-27 are rejected on the ground of non-statutory obviousness-type double patenting as being allegedly unpatentable over claims 1-4, and 6-17 of U.S. Patent No. 8,352,730.

3. Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AlA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention, or for pre-AlA the applicant regards as the invention.

4. Claims 1-2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,41, hereinafter "Hsu") Stanko (US Published App 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (US Published App 2002/0129262, hereinafter "Kutaragi").

5. Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

6. Claim 15 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (US Published App 2004/0129787, hereinafter "Saito").

7. Claims 16, 18-19, and 21 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,410, hereinafter "Hsu") and Stanko (US Published App 2005/0074126, hereinafter "Stanko").

8. Claim 17 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

The rejections are traversed herein.

Response to Objections

Claims 15 and 16 are objected to for alleged informalities.

With regard to claim 15, Applicant does not understand why "biometric scan" is objectionable and respectfully requests that the Examiner explain why "biometric scan" is objectionable.

With regard to claim 16, the Examiner appears to argue that line 5 should recite "comprise" rather than "comprises." It appears that recitation of "**the** other data values" has created ambiguity and confusion. "Plurality" modifies both the codes and other values (e.g. one code and one other data value, or two codes, or two other data values, etc.), so "the plurality … comprises the device ID code" is grammatically correct. This construction is supported by paragraph [0035], which teaches that, in one embodiment, "the code is a device ID." Similarly, "one or more" modifies both codes and other data values." Applicant has amended claim 16 and

the other claims to remove "the" where it precedes "other data values" in an attempt to remove the apparent confusion and ambiguity.

Response to Double Patenting Rejection

Claims 1-5, 7, 10-18, 22-24 and 26-27 are rejected on the ground of non-statutory double patenting as being allegedly unpatentable over claims 1-4 and 6-17 of U.S. Patent No. 8,352,730. Applicant does not acquiesce to the propriety of the double patenting rejection, but has submitted a terminal disclaimer with this amendment to advance prosecution. Accordingly, the Examiner is requested to withdraw the double patenting rejection.

Response to Rejections under 35 U.S.C. § 112

Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AlA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regard as the invention, or for pre-AlA the applicant regards as the invention.

Claims 1 and 24 are amended to correct the antecedent bases indicated by the Examiner. Claims 12 and 22 are amended to remove the "to" and "for" language that the Examiner based the section 112 rejection upon. Therefore, Applicant respectfully requests that the Examiner withdraw the section 112 rejection and allow the claims.

Response to Rejections under 35 U.S.C. § 103

Claims 1-2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,41, hereinafter "Hsu") Stanko (US Published

App 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (US Published App 2002/0129262, hereinafter "Kutaragi").

As amended, independent claim 1 recites in part:

> persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;
> responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan; . . .
> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality . . . wherein the one or more codes and other data values includes the device ID code; and
> receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

The claimed invention beneficially allows multiple levels of authentication to determine user access. Biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value are persistently stored in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, scan data from a biometric scan is received and compared to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, one or more of the plurality of codes and other data values, including a device ID code uniquely identifying the integrated device are wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code.

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on one or more of the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the one or more of the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing biometric data of a user … in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." The Examiner argues, on pages 14-15 of the OA, argues that Hsu teaches "persistently storing biometric data … in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." Specifically, the Examiner argues:

> persistently storing biometric data of the user and a plurality of codes and other data values a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered *(Figure 3, element 32, column 4, lines 15-25; column 7, lines 6-9, and 63-65); fob's public and private key pair, door's keying information, user's name, account number or other identifying information);*

Respectfully, the Examiner is incorrect. Hsu at most discloses "the device [of Hsu]… is highly resistant to reverse engineering … and other techniques for tampering" is not the same as "tamper proof" as "proof" by general definition indicates a greater degree of imperviousness

than "resistant." Moreover, even assuming a common definition of "highly resistant to tampering" and "tamper proof," Hsu does not suggest or disclose, among other things, that the format in which the information is stored is necessarily what makes the device of Hsu device highly resistant to tampering. For example, the high resistance to tampering may merely refer to the fact that the communications to/from the device of Hsu are encrypted thereby making it difficult to clone communications or reverse engineer the contents of the communication. Because Hsu fails to disclose or suggest that the format of the data stored on its device contributes to the device's high resistance to tampering, Hsu fails to disclose or suggest "persistently storing biometric data … in a tamper proof format… that is unable to be subsequently altered" as recited by claim 1.

Neither Stanko nor Kutaragi remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose storing biometric information in a tamper proof format. Applicant has search Kutaragi, and Kutaragi fails to mention biometrics, much less "persistently storing biometric data … in a tamper proof format." Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Moreover, the cited references fail to disclose or suggest "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered." The Applicant respectfully direct the Examiner to Hsu 5:19-21, which states:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For

Hence, Hsu discloses that biometric is **normally** not repeated unless the fob is lost or damaged. Hsu does not disclose or suggest, among other things, that enrollment is **unable** to be repeated absent the loss of or damage to the fob. Hsu discloses a common practice and not a feature/limitation of the fob. For example, the enrollment of Hsu may not **normally** be repeated unless the fob is lost or damaged because an individual's fingerprints remain relatively unchanged for long periods of time eliminating the desire to re-enroll and not because the person is unable to re-enroll biometric information. 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 further eliminating the potential for tampering.

Neither Stanko nor Kutaragi remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered," as recited by claim 1. Kutaragi fails to disclose or suggest biometrics, much less "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered," as recited by claim 1. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Applicant's claim 1 is patentable over the cited references for additional reasons. Applicant's invention biometrically verifies the user prior to using a third-party trusted authority

to authenticate the integrated device (based on one or more codes and other data values including the device ID code), and, responsive to successful authentication by the agent, allows the user access to an application. The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device.

Hsu at most discloses biometrically verifying the user at the integrated device before generating and encrypting a CRC based on the biometric information. The CRC is used for authentication at a door. A door is not a third-party trusted authority. In other words, Hsu does not provide two level authentication because Hsu verifies biometric information only (encryption does not necessarily verify the integrated device itself) and access is allowed/disallowed by the "door" without using a third-party trusted authority. Applicant's integrated device verifies both biometric data and the integrated device itself, and requires authentication by a third-party trusted authority.

Stanko does not disclose or suggest verifying biometric data prior to verifying the integrated device. Stanko discloses that an authentication server receives credentials, which may include biometrics, and the authentication server verifies the received credentials. Stanko, therefore, does not disclose verifying an integrated device itself nor does Stanko disclose verifying biometric information prior to authenticating the integrated device itself at a third-party trusted authority.

Kutaragi fails to disclose a biometric, much less sending a device ID code after successful biometric verification.

The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent responsive to a successful biometric authentication as recited by claim 1. Therefore, claim one is patentably distinct from the cited references and allowance of claim 1 is requested.

As claims 2, 4-7 and 9-11 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 4-7 and 9-11. Therefore, claims 2, 4-7 and 9-11 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 12, 16 and 22 recite language similar to claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 12, 16 and 22. Accordingly, claims 12, 16 and 22 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claim 13 depend from claim 12, claim 13 is patentable over the cited references for at least the same reasons as claim 12 as well as the additional limitations it recites. Similarly, claims 23-27 and 29 depend from claim 22, so claims 23-27 and 29 are patentable over the cited references for at least the same reasons as claim 22 as well as the additional limitations they recite. Hence, claims 1-2, 4-7, 9-13, 22-27 and 29 are patentably distinct from the cited references, whether alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

Claims 3 and 8 depend from claim 1, so all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to clams 3 and 8. Claim 14 depends from claim 12, so all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 14. Claim 20 depends from claim 16, so all arguments advanced above with respect to claim 16 are hereby incorporated so as to apply to clam 20. Claim 28 depends from claim 22, so all arguments advanced above with respect to claim 22 are hereby incorporated so as to apply to clam 28. Therefore, claims 3, 8, 14, 20 and 28 are patentable over Hsu, Stanko and Kutaragi.

Schlotterbeck fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Schlotterbeck at most disclose that a patient ID holds information such as age. *See* Schlotterbeck, ¶[0057]. Therefore, the cited portions of Schlotterbeck fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Moreover, holding an age does not disclose age verification,; therefore, claims 3 and 14 are patentable over Schotterbeck for at least this reason. Accordingly, withdrawal of the rejection is respectfully requested.

Claim 15 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (US Published App 2004/0129787, hereinafter "Saito").

As claim 15 depends from claim 12, all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 15. Therefore, claim 15 is patentable over Hsu, Stanko and Kutaragi. Saito fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Saito at most disclose that an LED provides visible feedback to the user. *See* Stanko, ¶[0041]. Therefore, the cited portions of Saito fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 16, 18-19, and 21 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,410, hereinafter "Hsu") and Stanko (US Published App 2005/0074126, hereinafter "Stanko").

As mentioned above, independent claim 16 recites language similar to claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claim 16. Accordingly, claim 16 is patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested. Claims 18-19 and 21 depend from claim 16 and are, therefore, patentable for at least the same reasons in addition to the other patentable elements they recite. Therefore, claims 16, 18-19, and 21 are patentably distinct from the cited references and withdrawal of their rejection is respectfully requested.

Claim 17 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

Claim 17 depends from claim 16, so all arguments advanced above with respect to claim 16 are hereby incorporated so as to apply to clam 17. Therefore, claim 17 is patentable over Hsu, Stanko and Kutaragi. As explained above, Schlotterbeck fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Accordingly, withdrawal of the rejection is respectfully requested.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: September 13, 2013 By: /Matthew Holmes/

Matthew Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net

EXHIBIT 9

WTS
ARTICLE DELIVERY

WTS Number: 348355

Order #199671

Economy

Request Date: 09/05/2024 03:50pm

Requester: DLA Piper Document Retrieval - DLA Piper

Delivery email: **documentretrievalteam@dlapiper.com**

Reference: 337722.000299 / Rob Williams / #269939 RS

Instructions: **I'd like to receive definitions from 10 technical dictionaries from different publishers from before 2005. If there are not 10 technical dictionaries with definitions for a particular term, just send as many as you have. Please make sure to include definitions from the IEEE dictionary and the Microsoft Computer Dictionary, to the extent the terms are found in those dictionaries. Please also send me definitions from the following traditional dictionaries from before 2005: Merriam-Websters, American Heritage and Oxford.**

WTS staff contact: Karen

Citation:

Definitions:
"tamper"
"tamper proof"
Specific Titles:
Dictionary Count: Subject: 10 Technical and the specified general dictionaries above
Date: Before 2005
Do not scan the page where the term would have appeared

4.Wiley Electrical and Electronics Engineering Dictionary

Library/Supplier: Memorial - WTS Collection
SCI 2004-02

ISSN/ISBN/OCLC: 0471402249

An outreach service of the General Library System, University of Wisconsin - Madison
http://wts.wisc.edu | wts@library.wisc.edu | 608.262.5917

er
Inc.

nary

ionary

hed by

WILEY ELECTRICAL AND ELECTRONICS ENGINEERING DICTIONARY

Steven M. Kaplan
Lexicographer

IEEE
IEEE PRESS

WILEY-INTERSCIENCE

A JOHN WILEY & SONS, INC., PUBLICATION

Copyright © 2004 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic format.

Library of Congress Cataloging-in-Publication Data is available.

Kaplan, Steven M.

Wiley Electrical and Electronics Engineering Dictionary

ISBN 0-471-40224-9

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

rmation in the form of a table.
orm another calculation on a col-

ves to read information from an
h as punched cards or perforated
calculations, lists, or the like.
ce into tables, or to calculate val-

rminal Access Controller Access
ntication protocol in which an ac-
with an authentication server to
to a network will be granted.
:en superseded by TACACS+,

version of **TACACS**, which in-
d a challenge/response system.
ACS+ is not compatible with

air navigation. An air navigation
and range information using UHF

neter.
trument which measures and indi-
hen graduated in revolutions per
meter. Its abbreviation is **tach**.
generator whose output energy is
onal speed of a connected shaft.
it energy may also be proportional

rticle whose speed would exceed

e as **tacan**.
sed on the sense of touch. Also

as **tactile sensor**.
t detects objects through physical
sensors may be used in robots, for
location, identity, and orientation
Also called **tactile sensing device**.
hone answering device.
mark or otherwise enable monitor-
example, a radioactive tracer, or
k, monitor, or identify with such a
or characters which serve to iden-
database. Also, the name of such
code which specifies how a docu-
ent, must be formatted. Examples
meta tags. Also, to so mark a
ler within an RFID system. Such a
he form of an IC, and responds to
ing from an RFID reader. Such a
incorporated into a box label, a
ain wand which is waved near a
Also called **RFID tag**.
nguage, such as HTML or XML,
3).
tag random-access memory. A
ch holds addresses, and which de-
emory which can be cached.
witching technology that uses **tags**
ormation.
Same as **TIFF**.
national Atomic Time.
lowest part of something. **2.** That
, bottom, or lowest part of some-
hat follows, and is in the same di-

rection as the main pulse that produced it. **4.** Same as **trailing edge**. **5.** A brief signal that remains after the actuating signal is removed. For example, a brief signal emitted by a transmitter after talking has stopped.

tailing An unwanted prolongation in the decay of a signal. In fax, or example, this may manifest itself as a tail that forms on the lines in the recorded copy. Also called **hangover** (2).

take-down Same as **takedown**.

take-down time Same as **takedown time**.

take-up reel In a tape player or system, the reel which winds the tape after it is played or recorded upon. The **supply reel** holds the tape before reproduction or recording. Also spelled **takeup reel**.

takedown After an operating cycle, the series of operations required to prepare a component, circuit, device, piece of equipment, system, material, or mechanism for the next cycle. Also spelled **take-down**.

takedown time The time interval required to complete a **takedown**. Also spelled **take-down time**.

takeup reel Same as **take-up reel**.

talk battery The DC voltage, typically 48V, which a central office supplies via the local loop for operation of a telephone. The ring voltage is usually higher.

talk-listen switch In an intercom or similar device, a switch that changes from the transmitting to the receiving mode, and vice versa. When a single speaker is used, it also serves to change to and from its microphone function.

talk power The power of an audio signal that is within the speech frequencies. Also called **speech power**, or **voice power**.

talk time The length of time a cell phone can be utilized for conversations. Usually expressed in minutes or hours. Also spelled **talktime**.

talker A command-driven technology which enables multiple users to interact with each other over the Internet, and which is utilized especially for real-time chatting.

talktime Same as **talk time**.

TAM Abbreviation of **telephone answering machine**.

tamper **1.** A material which is placed around the core of a nuclear reactor to reflect neutrons back to said core, preventing their escape. Also called **reflector** (4). **2.** To interfere in a harmful or unauthorized manner. For example, to tamper with a delicate mechanism without the proper expertise.

tamper-evident A security feature which makes any **tampering** evident. Used, for instance, to help protect smart cards against fraudulent reprogramming.

tamper-proof Not allowing, or impervious to **tampering**. It is very difficult to attain such a degree of protection.

tamper-resistance **1.** The property or characteristic of affording a comparatively high degree of protection against **tampering**. **2.** The extent to which something provides **tamper-resistance** (1).

tamper-resistant That which is characterized by **tamper-resistance**.

tamper switch A switch that is activated when something is interfered with in a harmful or unauthorized manner. Such a switch, for instance, may activate an alarm to indicate that a security mechanism is being meddled with.

tampering The process of interfering in a harmful or unauthorized manner. Said, for instance, of the improper use or alteration of a component, circuit, device, piece of equipment, system, material, or mechanism.

tan Abbreviation of **tangent** (1).

tandem The connection of circuits or devices in a manner that the output of one is the input of the next. Seen, for example in a cascade amplifier. Also called **cascade** (3).

tandem office A central office utilized mainly to connect trunks, as opposed to subscriber lines.

tandem office switch Same as **tandem switch**.

tandem processors Two or more processors utilized or connected together. Used, for instance, to provide fault-tolerance, or for multiprocessing.

tandem switch A central office switch utilized mainly to connect trunks, as opposed to subscriber lines. Also called **tandem office switch**.

tangent **1.** For a right triangle, the ratio of the length of the side opposite to an acute angle, to the length of the side adjacent to said acute angle. It is the same as the ratio of the sine to the cosine. Its abbreviation is **tan**. **2.** A line, curve, or plane which touches another curve or surface at a single point, but does not intersect it.

tangent galvanometer A galvanometer whose readings are proportional to the tangent of the angle of deflection of a needle from its position when no current is present.

tangential mode The reflection of sound waves off four of the six surfaces of a room.

tank **1.** Same as **tank circuit**. **2.** An acoustic delay line, such as a mercury delay line, which uses a recirculating fluid as the transmission medium. **3.** A capsule or container which holds a liquid. For example, that holding a pool of mercury in a mercury switch. **4.** A large container or reservoir for storing or holding fluids.

tank circuit Also called **tank** (1). **1.** A resonant circuit in which a capacitor and an inductor are connected in parallel with an AC source. Resonance occurs at or near the maximum impedance of the circuit. Also called **antiresonance circuit**, or **parallel-resonant circuit**. **2.** A circuit, such as a **tank circuit** (1), which serves to store energy. **3.** A **tank circuit** (2) which stores energy over a band of frequencies distributed around the resonant frequency.

tantalum A blue-gray hard metallic chemical element whose atomic number is 73. It has over 30 known isotopes, of which one is stable. It is more corrosion-resistant than platinum, it is very ductile, and can be drawn into very thin wires. Its applications in electronics include its use in semiconductors, lasers, analytical instruments, capacitors, vacuum tubes, and in alloys which provide very high corrosion resistance, ductility, and strength. Its chemical symbol is **Ta**.

tantalum capacitor An electrolytic capacitor in which the anode is composed of a tantalum foil, bar, or slug. Also called **tantalum electrolytic capacitor**.

tantalum carbide A crystalline solid nearly as hard as diamond, and whose chemical formula is **TaC**. It is used in electrodes, and objects requiring extreme resistance to corrosion and high strength, such as certain cutting tools.

tantalum chip capacitor A tantalum capacitor constructed in chip form. These are very small, and are used, for instance, in hybrid ICs.

tantalum electrolytic capacitor Same as **tantalum capacitor**.

tantalum oxide A white crystalline solid whose chemical formula is Ta_2O_5. It is used in lasers, semiconductors, optics, capacitors, and as a dielectric. Also called **tantalum pentoxide**.

tantalum pentoxide Same as **tantalum oxide**.

tap **1.** A connection made to a component, circuit, bus, or the like, at a point other than an end. Also, to make such a connection. **2.** A **tap** (1) utilized to connect a node to a network. **3.** A device that cuts internal threads, such as those of a screw. Also, to make such cuts. **4.** A concealed device which serves to surreptitiously intercept a communication, especially a telephonic conversation. Also called **wiretap** (1). **5.** To install a **tap** (4), or make such a connection. Also

This material may be protected by Copyright law (Title 17 U.S. Code)

EXHIBIT 10

WTS ARTICLE DELIVERY

WTS Number: 348352

Order #199671

Economy

Request Date: 09/05/2024 03:50pm

Requester: DLA Piper Document Retrieval - DLA Piper

Delivery email: **documentretrievalteam@dlapiper.com**

Reference: 337722.000299 / Rob Williams / #269939 RS

Instructions: **I'd like to receive definitions from 10 technical dictionaries from different publishers from before 2005. If there are not 10 technical dictionaries with definitions for a particular term, just send as many as you have. Please make sure to include definitions from the IEEE dictionary and the Microsoft Computer Dictionary, to the extent the terms are found in those dictionaries. Please also send me definitions from the following traditional dictionaries from before 2005: Merriam-Websters, American Heritage and Oxford.**

WTS staff contact: Karen

Citation:

Definitions:
"tamper"
~~"tamper proof"~~
Specific Titles:
Dictionary Count: Subject: 10 Technical and the specified general dictionaries above
Date: Before 2005
Do not scan the page where the term would have appeared

1. IEEE 100

Library/Supplier: IEEE

ISSN/ISBN/OCLC: 0-7381-2601-2

IEEE 100
The Authoritative Dictionary of IEEE Standards Terms

Seventh Edition

IEEE
Published by
Standards Information Network
IEEE Press

Authorized licensed use limited to: University of Wisconsin. Downloaded on April 30,2020 at 14:31:25 UTC from IEEE Xplore. Restrictions apply.

Short
Stand
Long

Case 6:24-cv-00143-ADA Document 46-10 Filed 11/05/24 Page 4 of 5

Trademarks and disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

Other tradenames and trademarks in this document are those of their respective owners.

The Institute of Electrical and Electronics Engineering, Inc.
3 Park Avenue, New York, NY, 10016-5997, USA

Copyright © 2000 by the Institute of Electrical and Electronics Engineers, Inc. All rights reserved. Published December 2000. Printed in the United States of America.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

To order IEEE Press publications, call 1-800-678-IEEE.

Print: ISBN 0-7381-2601-2 SP1122

See other standards and standards-related product listings at: http://standards.ieee.org/

The publisher believes that the information and guidance given in this work serve as an enhancement to users, all parties must rely upon their own skill and judgement when making use of it. The publisher does not assume any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed.

This work is published with the understanding that the IEEE is supplying information through this publication, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. The IEEE is not responsible for the statements and opinions advanced in this publication.

Short
Stand
Long

Authorized licensed use limited to: University of Wisconsin. Downloaded on April 30,2020 at 14:31:25 UTC from IEEE Xplore. Restrictions apply.

Case 6:24-cv-00143-ADA Document 46-10 Filed 11/05/24 Page 5 of 5
This material may be protected by Copyright law (Title 17 U.S. Code)

of tagged frames: *VLAN-tagged frames* and *priority-tagged frames*. (C/LM) 802.1Q-1998

tag header Allows user priority information, and optionally, VLAN identification information, to be associated with a frame. (C/LM) 802.1Q-1998

tag line A control line, normally manila or synthetic fiber rope, attached to a suspended load to enable a worker to control its movement. *Synonym:* tag rope. (T&D/PE) 524-1992r

tag rope *See:* tag line.

tags Men-at-work tags of distinctive appearance, indicating that the equipment or lines so marked are being worked on. (T&D) C2.2-1960

Tag Set Name A numeric identifier associated with a set of security tags. (C/LM) 802.10g-1995

tag sort A sort that uses the address table sorting technique. (C) 610.5-1990w

tail (x-ray energy spectrometers) (on a monoenergetic peak) Any peak shape distortion that does not comply with the limits defining the full energy peak intensity and that does not come from a source of radiation other than the monoenergetic source in question. (NPS/NID) 759-1984r

tailing (1) (hangover) (facsimile) The excessive prolongation of the decay of the signal. *See also:* facsimile signal. (COM) 168-1956w

(2) (hydrometallurgy and ore concentration) (electrometallurgy) The discarded residue after treatment of an ore to remove desirable minerals. *See also:* electrowinning. (PE/EEC) [119]

tailing time (charged-particle detectors) (of an amplifier output pulse) The time interval between the top centerline of a unipolar pulse and the one percent level on the last transition. (NPS) 300-1988r

tail lamp (illuminating engineering) A lighting device used to designate the rear of a vehicle by a warning light. (EEC/IE) [126]

tail-of-wave (chopped wave) impulse test voltage (insulation strength) The crest voltage of a standard impulse wave that is chopped by flashover at or after crest. (PE/TR) 21-1976

tailrace The exit channel of water from the powerhouse. (PE/EDPG) 1020-1988r

tail recursive A property of the implementation of a programming language. In a tail-recursive implementation, iterative processes can be expressed by means of procedure calls. (The process described by a program is iterative if and only if the order of its space growth is constant, aside from that used for the values of the program's variables.) (C/MM) 1178-1990r

tailwater The water in the tailrace. (PE/EDPG) 1020-1988r

take-over time (T_T) Time taken to switch from one transmission direction to the other in double talk conversation on a handsfree telephone (HFT). The signal in the first direction is continuously applied while the interrupting signal is applied in the opposite direction. T_T is measured from the application of the interrupting signal until the output level due to the interrupting signal reaches 3 dB below its final value. (COM/TA) 1329-1999

takeup reel *See:* reel winder.

talker A node that sends an isochronous subaction for an isochronous channel. (C/MM) 1394-1995

talker echo Echo that reaches the ear of the talker. (EEC/PE) [119]

talker sidetone The sidetone acoustic output of the telephone caused by an input from the artificial mouth. (COM/TA) 269-1992

talking key A key whose operation permits conversation over the circuit to which the key is connected. (EEC/PE) [119]

talk-ringing key (listening and ringing key) A combined talking key and ringing key operated by one handle. (EEC/PE) [119]

tamper To interfere with the performance of a security sensor or the electrical connections within an alarm communications system. (PE/NP) 692-1997

tampering Attacks to physical and logical system components (i.e., hardware, software, media), including substituting rogue components in place of legitimate components, physical theft of components, damage to components, and electrical probing within the system. This threat area assumes that an intruder has physical or electrical access to the system components and their internal structure (e.g., processor and memory boards, software modules). (C/BA) 896.3-1993w

tamper protection 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. *See also:* quadrant. (C/BA) 896.3-1993w

tamper-resistant enclosure A metal-enclosure for a power switchgear assembly that is designed to resist damage to or improper operation of the switchgear from willful acts of destruction and which is designed to provide reasonably safe protection against tampering by unauthorized persons who may attempt to gain entry by forcible means, to insert foreign substances into, or otherwise tamper with the assembly. (SWG/PE) C37.20-1968w

tandem (cascade) (networks) Networks are in tandem when the output terminals of one network are directly connected to the input terminals of the other network. *See also:* network analysis. (CAS) [13]

tandem blocking The first and final failure matching loss for trunk-to-trunk connections. *See also:* matching loss. (COM/TA) 973-1990w

tandem central office (tandem office) A central office used primarily as a switching point for traffic between other central offices. (SWG/PE) C37.20-1968w

tandem-completing trunk A trunk, extending from a tandem office to a central office, used as part of a telephone connection between stations. (EEC/PE) [119]

tandem control (electric power system) A means of control whereby the area control error of an area or areas A, connected to the interconnected system B only through the facilities of another area C, is included in control of area C generation. (PE/PSE) 94-1970w

tandem drive Two or more drives that are mechanically coupled together. *See also:* electric drive. (IA/ICTL/APP/IAC) [69], [60]

tandem office (telephone switching systems) An intermediate office used primarily for interconnecting end offices with each other and with toll connecting trunks. (COM) 312-1977w

tandem trunk (data transmission) A trunk extending from a central office or a tandem office to a tandem office and used as part of a telephone connection between stations. (PE) 599-1985w

tangential plane The plane that is tangential to the surface of the VDT screen at the center-center point. (EMC) 1140-1994r

tangential wave path (data transmission) In radio wave propagation over the earth, a path of propagation of a direct wave, which is tangential to the surface of the earth. The tangential wave path is curved by atmospheric refraction. (PE) 599-1985w

tangent-plane approximation *See:* Kirchhoff approximation.

tank (storage cell) A lead container, supported by wood, for the element and electrolyte of a storage cell. *Note:* This is restricted to some relatively large types of lead-acid cells. *See also:* battery. (EEC/PE) [119]

tank circuit (signal-transmission system) A circuit consisting of inductance and capacitance, capable of storing electric energy over a band of frequencies continuously distributed about a single frequency at which the circuit is said to be resonant, or tuned. *Note:* The selectivity of the circuit is proportional to the ratio of the energy stored in the circuit to the

Short
Stand
Long

Authorized licensed use limited to: University of Wisconsin. Downloaded on April 30,2020 at 14:31:25 UTC from IEEE Xplore. Restrictions apply.

EXHIBIT 11

WTS

ARTICLE DELIVERY

WTS Number: 348363

Order #199671

Economy

Request Date: 09/05/2024 15:52

Requester: DLA Piper Document Retrieval - DLA Piper

Delivery email: **documentretrievalteam@dlapiper.com**

Reference: 337722.000299 / Rob Williams / #269939 RS

Instructions: **I'd like to receive definitions from 10 technical dictionaries from different publishers from before 2005. If there are not 10 technical dictionaries with definitions for a particular term, just send as many as you have. Please make sure to include definitions from the IEEE dictionary and the Microsoft Computer Dictionary, to the extent the terms are found in those dictionaries. Please also send me definitions from the following traditional dictionaries from before 2005: Merriam-Websters, American Heritage and Oxford.**

WTS staff contact: Karen

Citation:

Definitions:
"tamper"
"tamper proof"
Specific Titles:
Dictionary Count: Subject: 10 Technical and the specified general dictionaries above
Date: Before 2005
Do not scan the page where the term would have appeared

American Heritage College Dictionary - 4th ed.

Library/Supplier: Memorial - WTS Collection
GEN 2004-02

ISSN/ISBN/OCLC: 0618453008

An outreach service of the General Library System, University of Wisconsin - Madison
http://wts.wisc.edu | wts@library.wisc.edu | 608.262.5917

The American Heritage® College Dictionary

FOURTH EDITION

Houghton Mifflin Company
Boston • New York

The I
Colleg
colleg
marks
Herit
sible
more
that
brows
An
with
tainin
Diction
well a
on a
more

New V
al-Qae
WiFi. T
that n
Fourth
tool y
net te
rorism
the la
world.

Autho
Based
Usage
invalu
conun
hopefull
such a

Words are included in this Dictionary on the basis of their usage. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks. No investigation has been made of common-law trademark rights in any word, because such investigation is impracticable. The inclusion of any word in this Dictionary is not, however, an expression of the Publisher's opinion as to whether or not it is subject to proprietary rights. Indeed, no definition in this Dictionary is to be regarded as affecting the validity of any trademark.

American Heritage® and the eagle logo are registered trademarks of Forbes Inc. Their use is pursuant to a license agreement with Forbes Inc.

Copyright © 2004, 2002 Houghton Mifflin Company. All rights reserved.

No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without the prior written permission of Houghton Mifflin Company unless such copying is expressly permitted by federal copyright law. Address inquiries to Reference Permissions, Houghton Mifflin Company, 222 Berkeley Street, Boston, MA 02116.

ISBN 0-618-45300-8

Visit our website: www.houghtonmifflinbooks.com

The American Heritage college dictionary.-- 4th ed.
p.cm.
Based on the fourth ed. of the American Heritage dictionary.
ISBN 0-618-09848-8 (thumb edge) --
ISBN 0-618-19604-8 (deluxe binding)
1. English language--Dictionaries. 2. Americanisms. I Houghton Mifflin Company. II. American Heritage dictionary.

PE1628 .A6227 2002
423--dc21

2001039826

Manufactured in the United States of America

APL-PROXENSE_01138856

This material may be protected by Copyright law (Title 17 U.S. Code)

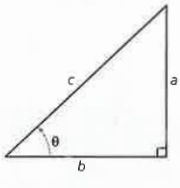
•er, -i•est 1. Talkative; loquacious. 2. Con-
o much talk. —talk'i•ness n.
, tall•est 1a. Having greater than ordinary
nsiderable height, esp. in relation to width;
ecified height. 3. Informal Fanciful or exag-
Impressively great or difficult: a tall order. 5.
ine. ❖ adv. With proud bearing; straight.
OE getæl, swift.] —tall'ness n.
a occasional tax levied by the Anglo-Norman
s and royal towns. ❖ tr.v. -laged, -lag•ing,
on. [ME taillage < OFr. < taillier, to cut, tax.

'ə-hās'ē) The cap. of FL, in the NW part;
he Florida Terr. in 1824. Pop. 150,624.
l'ə-hāch'ē) A river rising in N MS and flow-
ni) generally SW to the Yazoo R.
ə-pōō'sə) A river rising in NW GA and flow-
ni) to the Coosa R.
. Chiefly British A highboy.
•gord (tăl'ē-rănd'pĕr'ī-gôr', tä-lē-rän-pä-
aurice de 1754–1838. French public official
Revolution, Napoleon's reign, the Bourbon
reign of Louis Philippe.
n (tăl'ĭn, tä'lĭn) The cap. of Estonia, in the
f of Finland. Pop. 447,672.
(tăl'ĭs, tä-lēt') n., pl. tal•lith•im (tä-lē'sĭm,
tal•liths also tal•li•sim (tä-lē'sĭm, -lä'-) Ju-
tizith traditionally worn by Jewish males, esp.
yer. [Mishnaic Heb. tallīt, cover < Heb. tilēl,
lle! < ṭalāl, shade.]
A resinous liquid mixture of rosin acids and
as a byproduct in the treatment of pine pulp
emulsions, and lubricants. [Partial transl. of
l transl. of Swed. tallolja : tall, pine (< ON
e) + olja, oil.]
. Hard fat obtained from cattle, sheep, or
foodstuffs or to make candles, leather dress-
cants. 2. Any of various similar fats, such as
n plants. ❖ tr.v. -lowed, -low•ing, -lows 1.
with tallow. 2. To fatten (animals) to obtain
—tal'low•y adj.
-lies 1. A reckoning or score. 2a. A stick on
a count or score. b. A tally once used to keep
s paid or owed. 3. A mark used in recording a
bjects, most often in series of five, consisting
canceled diagonally or horizontally by a fifth
ng or classifying label, ticket, or piece of metal
rdens and greenhouses. 5. Something that is
esponds to something else; a double or coun-
-ly•ing, -lies —tr. 1. To reckon or count. 2.
g a mark. 3. Sports & Games To score (a point
r contest. 4. To label, as with a tally, for iden-
ication. 5. To cause to correspond or agree.
ce; correspond or agree. 2. To keep score. 3.
score a point or goal. [ME taly < AN tallie
Lat. tālea, stick.]
') interj. Used to urge hounds on during a fox
ho•ing, -hos —tr. To urge (hounds) on dur-
shouting "tallyho" when the fox is sighted.
llyho" as a hunting cry. ❖ n., pl. -hos 1. The
A fast coach drawn by four horses. [Prob. al-
t < OFr. thialau, taho.]
l, tăl'məd) n. Judaism The collection of an-
ings consisting of the Mishnah and the Ge-
the basis for much of Jewish law. [Mishnaic
ning, instruction < Heb. lāmad, to learn.]
mōō'dĭk, -myōō'-, tăl-), Tal•mu'di•cal (-dĭ-
l•ist (tăl'mōō-dĭst, tăl'mə-) n.
a. The claw of a bird of prey. b. The similar
animal. 2. Something similar to or suggestive
. 3. The part of a lock that the key presses in
olt. 4. Games The part of the deck of cards in
left on the table after the deal. 5. Architecture
[ME taloun < OFr. talon, heel < VLat. *talō,
ankle.]
l. -li (-lī') 1. The bone of the ankle that articu-
and fibula to form the ankle joint. 2. The
ankle.]
l. -lus•es A sloping mass of rock debris at a
< OFr. talu, earthwork slope < Lat. talātium,
p), perh. of Celt. orig.]
-o'-shanter.
) n. A Mexican dish made of fried chopped
peppers wrapped in cornhusks spread with
l. [< Am.Sp. tamales, pl. of tamal, tamale

-răk') n. A deciduous North American larch
having short needles borne on spur shoots.
rac, prob. of Algonquian orig.]
n•a•rao (tăm'ə-rou') n., pl. -raus also -raos
-black short-horned buffalo (Bubalus

mindorensis) of the island of Mindoro. [Tagalog tamaráw.]
ta•ma•ri (tə-mä'rē) n. Soy sauce made with little or no wheat. [J.]
tam•a•rin (tăm'ə-rĭn, -rän') n. Any of various small long-tailed arboreal monkeys of the genera Leontideus and Saguinus of Central and South America. [Fr. < Galibi.]
tam•a•rind (tăm'ə-rĭnd') n. 1. A tropical Asian evergreen tree (Tamarindus indica) having pinnately compound leaves, pale yellow flowers, and long pods containing small seeds embedded in an edible pulp. 2. The fruit of this tree. [ME < OFr. tamarinde < Ar. tamr hindī : tamr, dates + hindī, of India (< Pers. Hind, India; see HINDI).]
tam•a•risk (tăm'ə-rĭsk') n. Any of numerous African and Eurasian shrubs or small trees of the genus Tamarix, having small scalelike leaves. [ME tamarisc < LLat. tamariscus, var. of Lat. tamarix, tamaric-.]
Ta•ma•yo (tä-mä'yō), Rufino 1899–1991. Mexican artist whose works were influenced by pre-Columbian symbols.
tam•bour (tăm'bōōr', tăm-bōōr') n. 1. A drum or drummer. 2a. A small wooden embroidery frame consisting of two concentric hoops between which fabric is stretched. b. Embroidery made on such a frame. 3. A rolling front or top for a desk or table, consisting of narrow strips of wood glued to canvas. 4. Architecture See drum 3a. ❖ v. -boured, -bour•ing, -bours —tr. To do (embroidery) on a tambour. —intr. To embroider at or on a tambour. [ME < OFr., ult. < Ar. ṭanbūr, stringed musical instrument; prob. akin to Pers. tambūr, lute < MPers.]
tam•bou•ra or tam•bu•ra (tŭm-bōōr'ə) n. An unfretted lute of India and Turkey, used as a drone. [Urdu ṭambūra < Pers. ṭanbūra < Ar. ṭanbūr. See TAMBOUR.]
tam•bou•rin (tăm'bōō-rĭn, tăN-bōō-răN') n. 1a. A long, narrow, two-headed drum used in Provence. b. One who plays this drum. 2. A style of dance in lively two-beat rhythm, accompanied by this drum. [Provençal tambourin < OFr., dim. of tambour, tambour. See TAMBOUR.]
tam•bou•rine (tăm'bə-rēn') n. 1. A percussion instrument made up of a small drumhead with jingling disks fitted into the rim. 2. A similar instrument without a drumhead. [Fr. tambourin, small drum < OFr. See TAMBOURIN.]
Tam•bov (tăm-bôf', -bôv') A city of W Russia SE of Moscow; founded as a fortress in 1636. Pop. 293,000.
tam•bu•rit•za (tăm-bōōr'ĭt-sə, tăm'bə-rĭt'sə) n. A Balkan mandolinlike stringed instrument. [Serbo-Croatian tamburica, dim. of tambura, stringed instrument < Ottoman Turk. ṭambūra < Pers. ṭanbūra. See TAMBOURA.]
tame (tām) adj. tam•er, tam•est 1. Brought from wildness into a domesticated or tractable state. 2. Naturally unafraid; not timid. 3. Submissive; docile; fawning. 4. Insipid; flat: a tame party. 5. Sluggish; languid; inactive. ❖ tr.v. tamed, tam•ing, tames 1. To make tractable; domesticate. 2. To subdue or curb. 3. To tone down; soften. [ME < OE tam.] —tam'a•ble, tame'a•ble adj. —tame'ly adv. —tame'ness n. —tam'er n.
Tam•er•lane (tăm'ər-lān') or Tam•bur•laine (-bər-) 1336–1405. Mongolian conqueror of Persia, Turkey, and India.
Tam•il (tăm'əl, tŭm'-, tä'məl) n., pl. Tamil or -ils 1. A member of a Dravidian people of southern India and northern Sri Lanka. 2. The Dravidian language of the Tamil. ❖ adj. Of or relating to the Tamil or their language or culture. [Tamil.]
Tamm (täm), Igor Yevgeneevich 1895–1971. Russian physicist who shared a 1958 Nobel Prize.
Tam•muz also Tham•muz (tä'mōōz) n. The tenth month of the year in the Jewish calendar. See table at calendar. [Heb. tammūz; akin to Iraqi Ar. tabbūz, July, both ult. < Sumerian dumu-zi, Dumuzi, a dying and rising shepherd god : dumu, son + zi, true, effective.]
tam-o'-shan•ter (tăm'ə-shăn'tər) n. A Scottish cap or braided bonnet, sometimes having a pompon, tassel, or feather in the center. [After the hero of "Tam o' Shanter," a poem by Robert Burns.]
ta•mox•i•fen (tə-mŏk'sə-fĕn) n. A nonsteroidal estrogen antagonist used in the treatment and prevention of breast cancer. [T(RANS)- + AM(INO)- + alter. of OXY- + alter. of PHEN(OL).]
tamp (tămp) tr.v. tamped, tamp•ing, tamps 1. To pack down tightly by a succession of blows or taps. 2. To pack clay, sand, or dirt into (a drill hole) above an explosive. [Perh. back-formation < tampin, var. of TAMPION.]
Tam•pa (tăm'pə) A city of W-central FL on Tampa Bay, an inlet of the Gulf of Mexico. Pop. 303,000.
tam•per¹ (tăm'pər) v. -pered, -per•ing, -pers —intr. 1. To interfere in a harmful manner. 2. To tinker with something foolishly. 3. To engage in improper or secret dealings, as in an effort to influence. See Syns at interfere. —tr. To alter improperly. [Prob. alteration of TEMPER.] —tam'per•er n.
tamp•er² (tăm'pər) n. A neutron reflector in an atomic bomb that delays the expansion of the exploding material, making possible a longer-lasting and more energetic explosion.
Tam•pe•re (tăm'pə-rā', tăm'-) A city of SW Finland NNW of Helsinki. Pop. 202,000.
tam•per•proof (tăm'pər-prōōf') adj. Designed to prevent tampering or provide evidence of tampering.
Tam•pi•co (tăm-pē'kō, tăm-) A city of E-central Mexico near the Gulf of Mexico NNE of Mexico City. Pop. 295,000.
tam•pi•on (tăm'pē-ən) also tom•pi•on (tŏm'-) n. A plug or cover for the muzzle of a cannon or gun to keep out dust and moisture. [ME < OFr. tampon, var. of tapon, rag for stopping a hole, of Gmc. orig.]
tam•pon (tăm'pŏn') n. A plug of absorbent material inserted into a body cavity or wound to check a flow of blood or to absorb secretions, esp. one for the vagina during menstruation. [Fr. < OFr. See TAMPION.] —tam'pon' v.
tam-tam¹ (tŭm'tăm', tăm'tăm') n. A gong having a metal disk struck with a felt-covered hammer or stick, used in a gamelan orchestra. [Ult. of imit. orig.]
tam-tam² (tŭm'tăm', tăm'tăm') n. Variant of tom-tom.
tan¹ (tăn) v. tanned, tan•ning, tans —tr. 1. To convert (hide) into leather, as by treating with tannin. 2. To make brown by exposure to the sun. 3. Informal To thrash; beat. —intr. To become suntanned. ❖ n. 1. A light or moderate yellowish brown to brownish orange. 2. The brown color that sun rays impart to light skin. 3. Tanbark. 4a. Tannin. b. A solution derived from tannin. ❖ adj. tan•ner, tan•nest 1. Of the color tan. 2. Having a suntan. 3. Used in or relating to tanning. [ME tannen < OE *tannian < Med.Lat. tannāre < tannum, tanbark, prob. of Celt. orig.]
tan² abbr. Mathematics tangent
Ta•na (tä'nə, -nä) also Lake Tsa•na (tsä'-) A lake of NW Ethiopia; source of the Blue Nile.
tan•a•ger (tăn'ĭ-jər) n. Any of various small New World passerine birds of the family Thraupidae, often having brightly colored plumage in the males and usu. living in forests. [NLat. tanagra, alteration of Port. tangará < Tupi tanagorá.]
Tan•a•gra (tăn'ə-grə, tə-năg'rə) An ancient city of E-central Greece in E Boeotia; site of a Spartan defeat of Athenian forces in 457 B.C.
Ta•nakh (tä-näkн') n. The sacred book of Judaism, consisting of the Torah, the Prophets, and the Writings; the Hebrew Scriptures. [Acronym < the initial letters of the Heb. names for the Torah, the Prophets, and the Writings : t(ôrâ) + n(ə̂dî'îm) + k(ə̂tûbôt).]
Tan•a•na (tăn'ə-nō') A river of E and S AK flowing c. 764 km (475 mi) from the Wrangell Mts. to the Yukon R.
Ta•na•na•rive (tə-năn'ə-rēv', tä-nä-nä-rēv') See Antananarivo.
Tana River 1. A river of central Kenya flowing c. 805 km (500 mi) to the Indian Ocean. 2. A river, c. 322 km (200 mi), of NE Norway emptying into an inlet of the Arctic Ocean.
tan•bark (tăn'bärk') n. 1. The bark of various trees used as a source of tannin. 2. Shredded bark from which the tannin has been extracted, used to cover circus arenas and other surfaces.
Tan•cred (tăng'krĭd) 1078?–1112. Norman soldier who was a leader of the First Crusade (1096–99).
tan•dem (tăn'dəm) n. 1. A two-wheeled carriage drawn by horses harnessed one before the other. 2. A team of carriage horses harnessed in single file. 3. A tandem bicycle. 4. An arrangement of two or more persons or objects placed one behind the other. ❖ adj. Having two identical components arranged one behind the other. [Lat., at last, at length. See to- in App.]
tandem bicycle n. A bicycle built for two or more people sitting one behind the other.
tan•door (tăn-dōōr') n., pl. -doors or -door•i (-dōōr'ē) A cylindrical oven made of clay, heated to a high heat over charcoal or wood and used in India. [Hindi and Urdu tandūr < Pers., var. of tannūr < MPers. < Ar. < Akkadian tinūru, oven.]
tan•door•i (tăn-dōōr'ē) adj. Cooked in a tandoor. [Hindi tandūri < tandūr, tandoor. See TANDOOR.]
Ta•ney (tô'nē), Roger Brooke 1777–1864. Amer. jurist; chief justice of the US Supreme Court (1836–64).
tang¹ (tăng) n. 1. A distinctively sharp taste, flavor, or odor. 2. A distinctive quality that adds piquancy. 3. A trace, hint, or smattering. 4. A sharp point, tongue, or prong. 5. A projection by which a tool, such as a knife, is attached to its handle or stock. 6. A surgeonfish. ❖ tr.v. tanged, tang•ing, tangs 1. To furnish with a tang. 2. To give a tang to. [ME tange, of Scand. orig.] —tang'i•ness n. —tang'y adj.
tang² (tăng) n. A loud ringing sound; a twang. [Imit.] —tang v.
Tang (tăng) A Chinese dynasty (618–907) known for its wealth and its encouragement of the arts and literature.
Tan•gan•yi•ka (tăn'gən-yē'kə, tăng'-) A former country in E-central Africa; gained independence from Great Britain in 1961 and joined with Zanzibar to form Tanzania in 1964. —Tan'gan•yi'kan adj. & n.
Tanganyika, Lake A lake of E-central Africa between Congo (formerly Zaire) and Tanzania.
Tan•ge (tăn'gē), Kenzo 1913–2005. Japanese architect who designed the Peace Center and Park (1949–56) as part of the rebuilding of Hiroshima after World War II.
tan•ge•lo (tăn'jə-lō') n., pl. -los 1. A hybrid citrus tree derived from grapefruit and tangerine. 2. The aromatic fruit of this tree. [Blend of TANGERINE and POMELO.]
tan•gen•cy (tăn'jən-sē) also tan•gence (-jəns) n. The condition of being tangent.
tan•gent (tăn'jənt) adj. 1. Making contact at a single point or along a line; touching but not intersecting. 2. Irrelevant. ❖ n. 1.

tandoor



tangent
tan θ = a/b

ă	pat	oi	boy
ā	pay	ou	out
âr	care	o͝o	took
ä	father	o͞o	boot
ĕ	pet	û	cut
ē	be	ûr	urge
ĭ	pit	th	thin
ī	pie	*th*	this
îr	pier	hw	which
ŏ	pot	zh	vision
ō	toe	ə	about,
ô	paw		item

Stress marks:
' (primary);
' (secondary), as in
lexicon (lĕk'sĭ-kŏn')

EXHIBIT 12

Lineberry, Alice

From: Maxim Price <mprice@hechtpartners.com>
Sent: Friday, September 13, 2024 3:05 PM
To: Padmanabhan, Nandan; Lear Jiang; DLA-Apple-Proxense
Cc: Proxense-SG; Proxense
Subject: Re: Proxense v. Apple: Proxense's Proposed Claim Constructions

⚠ EXTERNAL MESSAGE

Counsel,

I write regarding the meet and confer discussed below.

1. The agreed-upon constructions listed in your email are accurate.
2. In addition, Proxense agrees to Apple's proposed grammatical changes to the construction for the "persistently storing" terms as follows:

'730 claims 1, 8 '954 patent, claim 1	"persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value … to a storage element" / "stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value … to the memory"	Plain and ordinary meaning, wherein the meaning is "persistently storing biometric data of the user and a plurality of codes and other data values to a storage element; within this storage element is also (1) a device ID code uniquely identifying the integrated device and (2) a secret decryption value" / Plain and ordinary meaning, wherein the meaning is "stores biometric data of the user and a plurality of codes and other data values to a memory; within this memory is also (1) a device ID code uniquely identifying the integrated device and (2) a secret decryption value"

3. In addition, we believe Apple's proposed construction for "tamper proof format" is accurate but only if the claim terms being construed are the full claim terms "tamper proof format... that is unable to be subsequently altered" and "tamper proof format.... that is not capable of being subsequently altered." As such, Proxense would agree to Apple's proposed construction ("a format that prevents any changes to the stored data") if the terms being construed are amended to include the full claim terms. Otherwise, the claims become redundant.
4. In addition, Proxense will agree that the preamble "A hybrid device comprising" is limiting.
5. You have requested from Proxense an identification of structure from the specification that Proxense would propose, in the alternative, for the "verification unit" term if that term is held to a be means-plus-function. We do not believe that there is any provision in the rules that requires Proxense to provide that structure ahead of its responsive claim construction brief. However, in the interest of professional courtesy, we will provide it subject to Proxense's reservation of its rights to amend this structure in response to Apple's arguments: Fig. 2; Fig. 4; Fig. 6; and Col. 3:47-4:3, 4:13-4:28.

In addition, based in part on the constructions of claim terms that have thus far been agreed upon between the parties in this thread and based on Proxense's ongoing evaluation of Apple's infringement, Proxense intends to move for leave to amend its complaint to withdraw the 188 patent and assert, in its stead, U.S. Patent Number US 9,679,289 claims 1 and 11. The infringement read for this patent will be substantially the same as the currently-asserted 042 patent and thus should not cause any delay. Nevertheless, we understand that Apple might want to take some time to review the 289 patent in the context of claim construction. As such, if Apple will not oppose Proxense's motion to amend, Proxense will agree to a reasonable extension of time for *Markman* briefing if the Court will permit it. That being said, this substitution should not create additional terms that need construction.

Best,
-Max
Maxim Price
Partner
Hecht Partners LLP

From: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>
Date: Wednesday, September 11, 2024 at 3:22 PM
To: Lear Jiang <LJiang@susmangodfrey.com>, DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Cc: Proxense-SG <sg-proxense@hechtpartners.com>, Proxense <proxense@hechtpartners.com>
Subject: RE: Proxense v. Apple: Proxense's Proposed Claim Constructions

Thanks all for the call. As discussed, can the Proxense team please let us know by Friday 9/13 about the following:

1. Whether there is agreement on Apple's proposed construction for the "persistently storing" term in the '730 patent family.
2. Proxense's alternative construction for "verification unit…" (including an identification of corresponding structure), which Proxense intends to advance to the extent the term if determined to be drafted in means-plus-function format.
3. Whether there is agreement that the preamble of claim 1 of the '042 patent and claim 1 of the '188 patent is limiting.

In addition, we discussed that both the Proxense and Apple teams would look into the rules regarding disclosure of rebuttal extrinsic evidence.

Finally, we understand that the parties' have reached agreement on the following constructions, but please let us know if you disagree:

8,352,730; 8,886,954; 9,298,905; 10,698,989 Patents		
Patent Claims	**Terms, Phrases or Clauses**	**Agreed Construction**
’730 claims 1, 8 ’954 claim 1 ’905 claim 1 ’989 claim 1	“device ID code” / “ID code” / “identification (ID) code”	A unique code identifying a device

8,6,46,042; 9,049,188 Patents		
Patent Claims	**Terms, Phrases or Clauses**	**Agreed Construction**
’042 patent claims 1, 6 ’188 patent claims 1, 3, 4, 7	“hybrid device”	a device comprising an integrated personal digital key (PDK) and an integrated receiver-decoder circuit (RDC)
’042 patent claims 1, 6 ’188 patent claim 1	“personal digital key (PDK)”	an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user
’042 patent claims 1, 6 ’188 patent claims 1, 3	“receiver-decoder circuit (RDC)”	a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing

Thanks,
Nandan

Nandan Padmanabhan
Partner

T +1 310 595 3082
F +1 310 595 3482
M +1 248 941 1828
nandan.padmanabhan@us.dlapiper.com

DLA Piper LLP (US)
dlapiper.com

From: Lear Jiang <LJiang@susmangodfrey.com>
Sent: Monday, September 9, 2024 5:39 PM
To: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>; DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Cc: Proxense-SG <sg-proxense@hechtpartners.com>; Proxense Hecht Partners <proxense@hechtpartners.com>
Subject: Re: Proxense v. Apple: Proxense's Proposed Claim Constructions

⚠ EXTERNAL MESSAGE

Hi Nandan,

We can meet at 11:30am PT on Wednesday. Can you circulate an invite?

Thanks,
Lear

From: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>
Date: Monday, September 9, 2024 at 10:40 AM
To: Lear Jiang <LJiang@susmangodfrey.com>, DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Cc: Proxense-SG <sg-proxense@hechtpartners.com>, Proxense Hecht Partners <proxense@hechtpartners.com>
Subject: RE: Proxense v. Apple: Proxense's Proposed Claim Constructions

EXTERNAL Email
Counsel,

The Court's schedule requires that we meet and confer regarding the claim terms in dispute and to exchange a revised list of terms/constructions. We are available to meet during the following time windows:

- Wednesday (9/11) between 11:30 am PT and 2:30 pm PT, or
- Thursday (9/12) between 9:30 am PT and 11 am PT, or 1:45 pm PT – 2:45 pm PT

Please let us know if any of these windows will work to discuss the claim terms.

Thanks,
Nandan

Nandan Padmanabhan
Partner

T +1 310 595 3082
F +1 310 595 3482
M +1 248 941 1828
nandan.padmanabhan@us.dlapiper.com

DLA Piper LLP (US)
dlapiper.com

From: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>
Sent: Tuesday, September 3, 2024 6:32 PM
To: Lear Jiang <LJiang@susmangodfrey.com>; DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Cc: Proxense-SG <sg-proxense@hechtpartners.com>; Proxense Hecht Partners <proxense@hechtpartners.com>
Subject: RE: Proxense v. Apple: Proxense's Proposed Claim Constructions

Counsel,

Please find attached Apple's proposed claim constructions for the terms previously identified.

Best,
Nandan

Nandan Padmanabhan
Partner

T +1 310 595 3082
F +1 310 595 3482
M +1 248 941 1828
nandan.padmanabhan@us.dlapiper.com

DLA Piper LLP (US)
dlapiper.com

From: Lear Jiang <LJiang@susmangodfrey.com>
Sent: Tuesday, September 3, 2024 6:30 PM
To: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>; DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Cc: Proxense-SG <sg-proxense@hechtpartners.com>; Proxense Hecht Partners <proxense@hechtpartners.com>
Subject: Proxense v. Apple: Proxense's Proposed Claim Constructions

⚠ EXTERNAL MESSAGE

Counsel,

Please see attached.

Thanks,
Lear

--
Lear Jiang | **Susman Godfrey L.L.P.**
1900 Ave. of the Stars, Ste. 1400
Los Angeles, CA 90067
310-789-3125 (o) | 330-475-5672 (c)

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

EXHIBIT 13

Lineberry, Alice

From: Lear Jiang <LJiang@susmangodfrey.com>
Sent: Tuesday, August 20, 2024 8:36 PM
To: Padmanabhan, Nandan; bmelton@SusmanGodfrey.com; Dhecht@hechtpartners.Com; sg-proxense@hechtpartners.com; proxense@hechtpartners.com
Cc: DLA-Apple-Proxense
Subject: Re: Case 6:24-cv-00143-ADA Proxense, LLC v. Apple, Inc. - Apple's Identification of Claim Terms for Construction

EXTERNAL MESSAGE

Counsel,

Pursuant to the scheduling order, Proxense does not believe that any claim terms for construction are needed beyond what the Court has already construed in the *Proxense v. Samsung*, *Proxense v. Google*, and *Proxense v. Microsoft* matters. Proxense believes the Court should adopt those prior constructions.

Thanks,
Lear
--
Lear Jiang | **Susman Godfrey L.L.P.**
1900 Ave. of the Stars, Ste. 1400
Los Angeles, CA 90067
310-789-3125 (o) | 330-475-5672 (c)

From: Padmanabhan, Nandan <nandan.padmanabhan@us.dlapiper.com>
Date: Tuesday, August 20, 2024 at 6:05 PM
To: Brian Melton <BMelton@SusmanGodfrey.com>, Lear Jiang <LJiang@susmangodfrey.com>, Dhecht@hechtpartners.Com <Dhecht@hechtpartners.Com>, sg-proxense@hechtpartners.com <sg-proxense@hechtpartners.com>, proxense@hechtpartners.com <proxense@hechtpartners.com>
Cc: DLA-Apple-Proxense <DLA-Apple-Proxense@us.dlapiper.com>
Subject: Case 6:24-cv-00143-ADA Proxense, LLC v. Apple, Inc. - Apple's Identification of Claim Terms for Construction

EXTERNAL Email
Counsel,

Pursuant to the schedule entered in this matter, please find attached Apple's identification of claim terms for construction.

Best,
Nandan

Nandan Padmanabhan
Partner

T +1 310 595 3082
F +1 310 595 3482
M +1 248 941 1828
nandan.padmanabhan@us.dlapiper.com

DLA Piper LLP (US)
2000 Avenue of the Stars
Suite 400 North Tower
Los Angeles, CA 90067-4704

DLA PIPER

dlapiper.com

The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please reply to the sender and destroy all copies of the message. To contact us directly, send to postmaster@dlapiper.com. Thank you.

EXHIBIT 14

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	13/710,109
FILING DATE:	December 10, 2012
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO:	10001-03653 US
CONFIRMATION NO:	5712

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Pacific Time Zone of the United States on the local date shown below:

Dated: April 2, 2014 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT B

Sir/Madam:

Responsive to the Office Action mailed on January 2, 2014, which sets a shortened statutory period for response that expires on April 2, 2014, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method comprising:

persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is ~~unable to be~~ not capable of being subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a third party that operates ~~by an agent that is~~ a ~~third-party~~ trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving, at an application, an access message from the ~~agent~~ trusted authority indicating that the ~~agent~~ trusted authority successfully authenticated the one or more codes and other data values sent to the third party and allowing the user access to [[an]]the application.

2. (Currently Amended) The method of claim 1, wherein the one or more codes and other data values are transmitted to the trusted authority ~~agent~~ over a network.

3. (Original) The method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

4. (Previously Presented) The method of claim 1, wherein the one or more codes and other data values indicate that the biometric verification was successful.

5. (Original) The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Original) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Original) The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. (Original) The method of claim 1, wherein the application includes a file including medical information.

9. (Original) The method of claim 1, wherein the application includes a financial account.

10. (Previously Presented) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and other data values for authentication.

11. (Previously Presented) The method of claim 1, further comprising:

receiving a request for the one or more codes and other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and other data values without a request for biometric verification, sending the one or more codes and other data values without requesting the scan data.

12. (Currently Amended) An integrated device comprising:

a persistent storage media that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage and ~~unable to be~~ not capable of being subsequently altered;

a verification module, coupled to communicate with the persistent storage, that receives scan data from a biometric scan for comparison against the biometric data, and that sends one or more codes and other data values from the plurality of codes and other data values for authentication by a third party that operates a trusted authority~~an agent~~, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module that receives an access message from the trusted authority~~agent~~ indicating that the trusted authority ~~agent~~ successfully

authenticated the one or more codes and other data values to the third party and allowing the user access to an application.

13. (Currently Amended) The integrated device of claim 12, wherein the one or more codes and other data values are transmitted to the trusted authority ~~agent~~ over a network.

14. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

15. (Original) The integrated device of claim 12 comprising:

an LED to be activated for requesting the biometric scan.

16. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

wirelessly receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with ~~an agent that is~~ a ~~third-party~~ trusted authority for authentication, the trusted authority operated by a third party;

requesting authentication of the integrated device using the one or more codes and other data values by the trusted authority~~agent~~;

receiving, at an application, an access message from the trusted authority ~~agent~~ indicating that the trusted authority ~~agent~~ successfully authenticated the one or more codes and other data values to the third party; and

in response to receiving the access message, allowing the biometrically verified user access to the ~~an~~ application.

17. (Currently Amended) The method of claim 16, further comprising:

registering a date of birth or age with the trusted authority~~agent~~.

18. (Previously Presented) The method of claim 16, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and other data values associated with the biometrically verified user is received from the integrated device.

19. (Original) The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (Original) The method of claim 16, wherein the application includes a file including medical information.

21. (Original) The method of claim 16, wherein the application includes a financial account.

22. (Currently Amended) A system, comprising:

an integrated hardware device that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element in the integrated device that is ~~unable to be~~ not capable of being

subsequently altered, and that wirelessly sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and other data values include the device ID code; and

an authentication unit that receives the one or more codes and other data values and sends the one or more codes and other data values to a third party that operates a trusted authority ~~an agent~~ for authentication, and that receives an access message from the trusted authority ~~agent~~ indicating that the trusted authority ~~agent~~ successfully authenticated the one or more codes and other data values to the third party and allows the user to access an application.

23. (Previously Presented) The system of claim 22, wherein the integrated device receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate scan data.

24. (Previously Presented) The system of claim 22, wherein when the integrated device cannot verify scan data as being from the user, the integrated device does not send the one or more codes and other data values.

25. (Original) The system of claim 22, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. (Original) The system of claim 22, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

27. (Original) The system of claim 22, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. (Original) The system of claim 22, wherein the application includes a file including medical information.

29. (Original) The system of claim 22, wherein the application includes a financial account.

REMARKS

Claims 1-29 were presented for examination. Claims 1-29 stand rejected in the Office Action dated January 2, 2014 (herein, "OA"). Claims 1, 2, 12, 13, 16, 17 and 22 are amended. Claims 1-29 are pending upon entry of this amendment.

Summary of Office Action

1. Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AIA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention, or for pre-AIA the applicant regards as the invention.

2. Claims 1, 2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (U.S. Patent No. 6,041,410, hereinafter "Hsu") Stanko (U.S. Publication No. 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (U.S. Publication No. 2002/0129262, hereinafter "Kutaragi").

3. Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (U.S. Publication No. 2004/0128162, hereinafter "Schlotterbeck").

4. Claim 15 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (U.S. Publication No. 2004/0129787, hereinafter "Saito").

5. Claims 16, 18, 19, and 21 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu and Stanko.

6. Claim 17 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck.

The rejections are traversed herein.

Interview Summary

On April 1, 2014, Applicant's representative, Matthew Holmes, had a telephonic interview with the Examiner and the Examiner's SPE and discussed the independent claims with regard to the cited references. The Applicant's representative was encouraged to amend the independent claims to clarify the third party, and the language "sending… to a third party that operates a trusted authority" was specifically suggested to the Applicant's representative to overcome the cited references. Column 5, lines 20-22 of Hsu were also discussed. Specifically, the presence of the term "normally" and its impact on Hsu's disclosure. The Applicant's representative was encouraged to amend the claims to read "not capable of being subsequently altered" rather than "unable to be subsequently altered" as previously presented. The independent claims are amended herein to include the suggested language. Therefore, the Applicant respectfully requests that the rejections be withdrawn and the claims allowed.

Response to Rejections under 35 U.S.C. § 112

Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AlA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention, or for pre-AlA the applicant regards as the invention.

Applicant has amended claims 12 and 22 as suggested by the Examiner on page 2 of the OA. Accordingly, the Applicant requests that the Examiner withdraw the section 112 rejection.

Response to Rejections under 35 U.S.C. § 103

Claims 1, 2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hsu et al. (U.S. Patent No. 6,041,410, hereinafter "Hsu") Stanko (U.S. Publication No. 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (U.S. Publication No. 2002/0129262, hereinafter "Kutaragi").

Independent claim 1 recites in part:

> persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is **not capable** of being subsequently altered …
> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and other data values for authentication to a **third party** that operates a trusted authority … ; and
> receiving, at an application, an access message …and allowing the user access to the application. (emphasis added)

The Examiner argues that "***unable*** to be subsequently altered" element of claim 1 is disclosed by Hsu. However, Hsu discloses "Enrollment … is not ***normally*** repeated unless the fob is lost or damaged" (emphasis added). *See* Hsu, Col. 5 Lines 20-22. Hsu does not disclose "Enrollment … is unable to repeated unless the fob is lost or damaged." As the Examiner herself indicates, on page 3 of the OA, "it does not make sense if enrollment is repeated on a lost or damaged fob." The word "normally" may indicate that the cited portion of the reference describes a normal use case of the fob not an actual limitation on the capability, or an inability, of the fob. Therefore, Hsu fails to explicitly or inherently disclose "***unable*** to be subsequently altered," as recited by previously presented claim 1.

The Applicant's point may be better demonstrated with the following example. Assume the Applicant states to the Examiner that the Applicant normally does not turn off his computer unless it is Friday evening. Presumably, the Examiner recognizes that this statement does not disclose that the Applicant's computer is unable to be turned off unless it is Friday evening or that the Applicant is somehow unable to turn the computer off unless it is Friday evening. In fact, the Applicant is able to turn the computer off at other times. The disclosure merely indicates a habit or custom, i.e., that the Applicant normally chooses not to turn of the computer at other times. Accordingly, there is a distinction between disclosing what is "normally" performed/not performed and disclosing what is able, or unable, to be performed. Examiner's SPE suggested that the language "not capable of being subsequently altered" may better capture the above distinction and the independent claims have been amended thusly.

Hsu's disclosure that enrollment is not normally repeated absent loss of or damage to the fob does not disclose that Hsu's fob is unable to repeat enrollment. At most, it discloses that repeating enrollment absent loss or damage to the fob is not "normal." This may be, for example, because fingerprints normally do not change significantly over time so repeating enrollment is not normally necessary and therefore "not normally repeated." Nothing in Hsu indicates that enrollment may not be repeated in an abnormal situation (e.g. repeating enrollment to enroll a finger from the user's left hand instead of the user's right hand because the user lost his/her right hand in a farming accident). In fact, the enrollment process of Hsu consists of flipping a switch on the device to an enrollment mode. Hsu col. 2, lines 10-14. Hsu does not disclose or suggest that this switch is unable to be flipped to repeat enrollment. While Hsu indicates that the fob is "highly resistant to reverse engineering, "cloning" and other techniques for tampering to obtain access to protected properties," *see* Hsu, Col. 7 Lines 63-65, Hsu does

not explicitly or inherently disclose that this high resistance is achieved because the enrollment process is unable to be repeated. Applicant points out that storing a hash of the fingerprint or encrypting the fingerprint would prevent reverse engineering or tampering to obtain the fingerprint (i.e. a protected property) regardless of whether that hash/fingerprint may be repeatedly altered, e.g., by overwriting it with a new fingerprint during re-enrollment. Hsu does not disclose that overwriting a first fingerprint of an authorized user with a second fingerprint of the authorized user constitutes reverse engineering, cloning, or other techniques to obtain access to the protected properties.

To summarize and simplify, Hsu at most discloses choosing not to alter under normal circumstances and Applicant teaches "**not capable** of being subsequently altered." Accordingly, Hsu fails to disclose or suggest, among other things, "**not capable** of being subsequently altered," as recited by claim 1. As Applicant discussed in the prior response, dated September 13, 2013, the other cited references fail to correct the deficiencies of Hsu, nor does the Examiner argue that they do. For this reason alone claim 1 is patentable over the cited references.

Additionally, claim 1 is amended to clarify the presence of a third party and its role in the authentication. Specifically, claim 1 recites "sending one or more codes and other values from the plurality of codes and other data values for authentication to a **third party** that operates a trusted authority," as amended. Hsu at most discloses a door matching a received CRC with a CRC in its database. *See* Hsu column 7, lines 30-34. The door is not a third party that operates a trusted authority. The other cited references do not remedy the deficiencies of Hsu nor does the Examiner argue that they do. Therefore, the cited references fail to disclose such a third party and claim 1 is patentable for at least this reason.

Therefore, the cited references whether taken alone or in combination fail to disclose or suggest each and every element of amended claim 1. Therefore, claim 1 is patentably distinct from the cited references and allowance of claim 1 is requested.

As claims 2, 4-7 and 9-11 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 4-7 and 9-11. Therefore, claims 2, 4-7 and 9-11 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 12 and 22 recite language similar to claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 12, 16 and 22. Accordingly, claims 12, 16 and 22 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claim 13 depend from claim 12, claim 13 is patentable over the cited references for at least the same reasons as claim 12 as well as the additional limitations it recites. Similarly, claims 23-27 and 29 depend from claim 22, so claims 23-27 and 29 are patentable over the cited references for at least the same reasons as claim 22 as well as the additional limitations they recite. Hence, claims 1-2, 4-7, 9-13, 22-27 and 29 are patentably distinct from the cited references, whether alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (U.S. Publication No. 2004/0128162, hereinafter "Schlotterbeck").

Claims 3 and 8 depend from claim 1, so all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to clams 3 and 8. Claim 14 depends from claim 12, so all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 14. Claim 28 depends from claim 22, so all arguments advanced above with respect to claim 22 are hereby incorporated so as to apply to clam 28. Therefore, claims 3, 8, 14 and 28 are patentable over Hsu, Stanko and Kutaragi for at least the reasons described above with reference to claim 1.

Schlotterbeck fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Schlotterbeck at most disclose that a patient ID holds information such as age. *See* Schlotterbeck, ¶[0057]. Therefore, the cited portions of Schlotterbeck fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Moreover, holding an age does not disclose age verification; therefore, claims 3 and 14 are patentable over Schotterbeck for at least this reason. Accordingly, withdrawal of the rejection is respectfully requested. Therefore, claims 3, 8, 14 and 28 are patentable over the cited references for at least the reasons described above with reference to claim 1.

Claim 20 depends from independent claim 16. Claim 16, as amended, recites in part:

> … *the device ID code being registered with a trusted authority* <u>*for authentication, the trusted authority operated by a third party*</u>; …
> 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 to the third party; … (emphasis added)

Claim 16 beneficially teaches that "*the device ID code [is] registered with a trusted authority* <u>*for authentication, the trusted authority operated by a third party*</u>." This beneficially allows the user to retain control of his/her biometric data as it is stored on his/her integrated device and not in a repository in "the cloud" that might be a lucrative target for getting hacked,

while providing the benefits of having third party identification. Support for the amendment may be found throughout the specification, for example, at paragraphs [0009] and [0049].

The Examiner argues on page 3 and elsewhere in the OA that Hsu's door reads on the "third-party trusted authority." However, the Examiner fails to address the "third-party" element of previously presented claim 1. Applicants amend the independent claims to clarify the presence of a "third party." Support for the amendment may be found throughout the specification, for example, at paragraph [0009].

Hsu at most discloses that "each door also has a database 52 in which is stored the user name, the user fob public encryption key and the user CRC, for each user registered to use the door." Hsu, col. 6, lines 31-34. Thus, Hsu does not disclose "*a trusted authority for authentication, the trusted authority operated by a third party*," as recited by claim 1.

Neither Stanko, nor Kutaragi nor Schlotterback remedy the deficient disclosure of Hsu. Applicant has searched Stanko for "*a trusted authority for authentication, the trusted authority operated by a third party*" and Stanko fails to disclose a "third party," much less "*a trusted authority for authentication, the trusted authority operated by a third party*." Applicant has search Kutaragi for "third party" and Kutaragi fails to mention a "third party," much less "*a trusted authority for authentication, the trusted authority operated by a third party*." Applicant has search Schlotterback for "third party" and Schlotterback fails to mention a "third party," much less "*a trusted authority for authentication, the trusted authority operated by a third party*." Therefore, claim 16 is patentably distinct from the cited references. Claim 20 depends from claim 16 and is therefore patentable for at least the same reason.

Claim 15 is rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (U.S. Publication No. 2004/0129787, hereinafter "Saito").

As claim 15 depends from claim 12, all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 15. Therefore, claim 15 is patentable over Hsu, Stanko and Kutaragi. Saito fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Saito at most disclose that an LED provides visible feedback to the user. *See* Stanko, ¶[0041]. Therefore, the cited portions of Saito fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 16, 18, 19, and 21 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hsu and Stanko.

As discussed above with reference to claim 20, independent claim 16 is patentable over Hsu and Stanko as well as Kutaragi and Schlotterbeck. Accordingly, claim 16 is patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested. Claims 18-19 and 21 depend from claim 16 and are, therefore, patentable for at least the same reasons in addition to the other patentable elements they recite. Therefore, claims 16, 18-19, and 21 are patentably distinct from the cited references and withdrawal of their rejection is respectfully requested.

Claim 17 is rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck.

Claim 17 depends from claim 16, so all arguments advanced above with respect to claim 16 are hereby incorporated so as to apply to clam 17. Therefore, as explained above, the cited references fail to disclose each and every element of claim 16. Therefore, claim 16 and its dependents are patentable over the cited references. Accordingly, withdrawal of the rejection is respectfully requested.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: April 2, 2014 By: /Kanda Ishihara/

Kanda V. Ishihara, Reg. No. 56,607
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (650) 537-4505
Fax: (801) 355-0160
Email: kishihara@patentlawworks.net

EXHIBIT 15

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC, *Plaintiffs*, v. SAMSUNG ELECTRONICS, CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC, *Defendants*.	Civil Action No. 6.21-CV-00210 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendants Samsung Electronics Co., Ltd. ("SEC") and Samsung Electronics America, Inc. ("SEA") (collectively, "Samsung" or "Defendants"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Samsung infringes one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. Upon information and belief, SEC is a corporation organized under the laws of the Republic of Korea, having a place of business at 129, Samsung-Ro, Yeongtong-Gu, Gyeonggi,

16677, Republic of Korea. SEC may be served with process pursuant to Federal Rule of Civil Procedure 4(f)(1).

4. Upon information and belief, SEA is a corporation organized under the laws of New York, having a principal place of business at 85 Challenger Rd., Ridgefield Park, NJ 97660. SEA maintains a place of business in this District at 12100 Samsung Blvd., Austin, TX 78754. SEA may be served with process through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, TX 75201.

5. SEC designs, manufactures, and provides to the United States and other markets a wide variety of hardware and software products and services, including consumer electronics, mobile phones, handheld devices, tablets, laptops and other personal computers, storage devices, televisions, and electronic devices.

6. Upon information and belief, SEA is a wholly-owned subsidiary of SEC and is responsible for domestic distribution of Samsung's consumer products, including the products accused of infringement herein.

JURISDICTION AND VENUE

7. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

8. This Court has personal jurisdiction over Samsung because it has conducted and continues to regularly conduct business within the State of Texas and this District. Samsung has purposefully and voluntarily availed itself of the privileges of conducting business in the United States, the State of Texas, and this District by continuously and systematically placing goods into

the stream of commerce through an established distribution channel with the expectation that they will be purchased by consumers in this District. Samsung directly and/or through intermediaries (including distributors, sales agents, and others), ships, distributes, sells, offers to sell, imports, advertises, makes, and/or uses its products (including but not limited to the products accused of infringement herein) in the United States, the State of Texas, and this District.

9. SEA is registered to do business in Texas and maintains an agent for service of process in Texas. SEA maintains places of business within the Western District of Texas, including at 12100 Samsung Blvd., Austin, TX 78754.

10. Upon information and belief, Samsung has authorized retailers that offer and sell products on its behalf in this District, including products accused of infringement herein. Upon information and belief, these include Walmart, *e.g.*, Supercenter #939, 4230 Franklin Ave., Waco, TX 76710; Target, *e.g.*, at 5401 Bosque Blvd., Waco, TX 76710; Best Buy, *e.g.*, at 4627 S. Jack Kultgen Expy., Waco, TX 76706; T-Mobile Store, *e.g.,* at 1107 N Valley Mills Dr., Bldg 1, Waco, TX 76710; and Verizon, *e.g.*, at 1820 S Valley Mills Dr., Waco, TX 76711, among many others.

11. Proxense's causes of action arise directly from Samsung's business contacts and other activities in the State of Texas and this District.

12. Samsung has derived substantial revenues from its infringing acts within the State of Texas and this District.

13. Venue is proper in this District as to SEC pursuant to 28 U.S.C. § 1391(c)(3) because it is not a resident of the United States and may therefore be sued in any judicial district.

14. Venue is proper in this District as to SEA pursuant to 28 U.S.C. § 1400(b) because SEA has committed acts of infringement in this District and has regular and established places of business in this District.

15. Joinder of SEC and SEA is proper because they are related entities that are either jointly and severally liable for infringement, or that make, use, sell, offer to sell, and/or import the same or similar products accused of infringement herein. Further, upon information and belief, SEC and SEA use the same underlying hardware and/or software in their infringing products and therefore the factual question of infringement will substantially overlap between SEC and SEA. Proxense anticipates there will be substantial overlap with respect to discovery.

16. Samsung has committed acts of infringement in this District and does business in this District, including making sales and/or providing service and support for customers and/or end-users in this District. Samsung purposefully and voluntarily sold one or more infringing products with the expectation they would be purchased in this District. These infringing products have been and continue to be purchased in this District. Thus, Samsung has committed acts of infringement within the United States, the State of Texas, and this District.

PATENTS-IN-SUIT

17. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 1**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=08352730.

18. On March 26, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,298,905 (the "905 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 905 Patent is attached hereto as **Exhibit 2**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09298905.

19. On June 30, 2020, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,698,989 (the "989 Patent") entitled "Biometric personal data key (PDK)

authentication." A true and correct copy of the 989 Patent is attached hereto as **Exhibit 3**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=10698989.

20. On June 2, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,049,188 (the "188 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 188 Patent is attached hereto as **Exhibit 4**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09049188.

21. On January 12, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,235,700 (the "700 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder circuit and Methods of Use." A true and correct copy of the 700 Patent is attached hereto as **Exhibit 5**, and also available at https://pdfpiw.uspto.gov/.piw?PageNum=0&docid=09235700.

22. Proxense is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the 730, 905, 989, 188, and 700 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

23. The technologies of the Patents-in-Suit were invented by John Giobbi and David L. Brown. The 730 and 905 Patents generally cover systems and methods for an integrated device that persistently stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (*e.g.*, a finger-print) can be compared against the stored biometric data. Once the user has been biometrically verified by the integrated device, a code can be wirelessly

transmitted for authentication. The 989 Patent generally covers systems and methods of verifying a user during authentication of an integrated device.

24. The 188 and 700 Patents generally covers a hybrid device including a personal digital key ("PDK") and receiver-decoder circuit ("RDC"), wherein the PDK and RDC are coupled for communication with each other. The 188 and 700 Patents also includes a number of system configurations for use of the hybrid device including: use of the hybrid device in a cell phone; simultaneous use of the PDK and the RDC functionality of hybrid device; use of multiple links of hybrid device to generate an authorization signal, use of multiple PDK links to the hybrid device to generate an authorization signal; and use of the hybrid device for authorization inheritance.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

25. Global contactless transaction values were estimated at $2 trillion in 2020. By 2024, they may reach $6 trillion according to forecasts. Mobile payments, or transactions initiated on mobile devices such as cell phones or tablet computers, have become increasingly popular as applications like Samsung Pay, launched in 2015, come bundled with Samsung's popular devices, like the Galaxy-branded line of phones. According to Samsung, "consumers have relied on Samsung Pay to make billions of transactions." Mobile payments can include payments for goods and services purchased over the internet (*e.g.,* through merchant websites or applications), or payments at a point of sale, which are payments initiated from a mobile device at a physical location.

26. Near Field Communication ("NFC") is a form of contactless communication between devices that allows two NFC-equipped devices placed within a few centimeters of each other to exchange data. NFC technology provides power consumption and ease-of-use advantages

as compared to other methods of close-proximity wireless communication (*e.g.*, Bluetooth). NFC can be used to facilitate mobile payments when an NFC-equipped device (such as a smartphone or electronic wearable like a watch) is placed near a contactless merchant terminal, allowing the devices to exchange payment data.

27. Contactless merchant terminal adoption in the U.S. has been expedited by card issuer security requirements. Card issuers in the United States set an October 2015 deadline for merchants to upgrade payment terminals capable of accepting credit cards with embedded chips for security, and many of these upgraded terminals have NFC capability built in. In December 2015, approximately 2.36 million contactless terminals were in service in the United States. As a result of the COVID-19 pandemic, there has been a sharp rise in adoption of contactless payment all over the globe.

28. Magnetic Secure Transmission ("MST") is a technology that emits a magnetic signal to mimic the magnetic strip on a traditional payment card. MST technology can be used to facilitate mobile payments when an MST-equipped device is placed near a merchant terminal, allowing the devices to exchange data. MST does not generally require merchants to upgrade payment terminal software or hardware. The technology was developed to facilitate contactless payments on point-of-sale terminals that can accept only conventional magnetic stripe cards. LoopPay, a contactless payments company that utilized MST (and was acquired by Samsung), claimed a 90% merchant acceptance rate.

II. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

29. Proxense was founded in 2001 as a limited venture. The company was formally incorporated in 2005 as an LLC. From approximately 2004-2012, Proxense developed, *inter alia*, mobile payment technologies and commercial products, employing over thirty engineers, and

investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

30. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of utilizing small electronic sensors, or receiver-decoder circuits ("RDCs"), capable of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

31. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including three of the asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

32. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 6**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), **Exhibit 7**.

33. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), **Exhibit 8**. The DARKReading article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

34. It would be years until products like Apple Pay (2014) and Samsung Pay (2015) were launched and became mainstream; Apple's TouchID, which involves fingerprint recognition technology, and Samsung's fingerprint scanner on its own phones, were introduced in 2013 and 2014, respectively. Accordingly, Proxense's technology was years ahead of the industry.

35. After the launch of services like Samsung Pay, and its inextricable link to the some of the most popular smartphone hardware devices in the United States, and the world, Proxense

would find itself unable to compete with companies like Samsung, even though Proxense invented the technology utilized in these solutions.

36. Today, Proxense holds at least 65 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management and mobile payments. Proxense continues to prosecute new patents on its proprietary technology.

III. INFRINGEMENT ALLEGATIONS

1. Proxense's Interactions with Samsung

37. In or around April 2017, Proxense was introduced to Samsung. Since at least that time, Samsung has had constructive notice of the Patents-in-Suit and the scope of their claims as of at least their dates of issue. Proxense has given Samsung actual notice of the Patents-in-Suit, and also placed Samsung on notice of the Patents-in-Suit as of the date of public filing of this Complaint.

38. Samsung has also had knowledge of the infringing nature of its activities, or at least a willful blindness regarding the infringing nature of its activities, since at least Proxense's making Samsung aware of the Patents-in-Suit, if not as of the public filing of this Complaint.

39. Despite Samsung's knowledge of the Patents-in-Suit, and its constructive knowledge of its infringing actions, Samsung continued to infringe the claims of the Patents-in-Suit. Samsung's infringement has been and continues to be willful since at least the date of the public filing of this Complaint.

2. The Accused Products

40. Samsung has manufactured, used, marketed, distributed, sold, offered for sale, and exported from and imported into the United States devices and software that directly and/or

indirectly infringe (literally or via the doctrine of equivalents) the Patents-in-Suit. Samsung has distributed variants of Samsung Pay that have included functionality to verify a user during authentication of a smartphone. Samsung Pay is operable on a range of Samsung devices, including at least all smartphones from the Galaxy S6 and above, including but not limited to, at least the Samsung devices set forth in **Appendix A**, including Galaxy S21, S20+, S21 Ultra, Galaxy S20, S20+, S20 Ultra 5G, Galaxy Fold, Galaxy Z-Flip, ZFlip 5G, Galaxy Note 20, Note 20 Ultra, Note10, Note10+, Note10+ 5G, Note5, Galaxy S10e, S10, S10+, Galaxy Note9, Galaxy S9, S9+, Galaxy Note8, Galaxy Note5, Galaxy S8, S8+, Galaxy S7, S7 edge, Galaxy S6, S6 edge, S6 edge+, S6 Active, Galaxy A90, Galaxy A80, Galaxy A70, A71, A71 5G, Galaxy A50, A51, Galaxy A40, Galaxy A30, A31, Galaxy A20e, Galaxy A8, Galaxy A7, Galaxy A5, Galaxy J7, Galaxy J5 Pro, Galaxy Watch S3, Galaxy Watch S2 Sport, Galaxy Watch S2 Classic, Gear S3 Frontier, Gear S3 Classic, Galaxy Watch Active 2, Galaxy Watch Active, Galaxy Watch, Gear Sport, Gear S3, and Gear S2, and all Samsung devices released since September 2015. The current and previous versions of Samsung Pay and devices with Samsung Pay, alone and together, are non-limiting instances of the Accused Products. The Accused Products practice the claims of the Patents-in-Suit to improve the shopping experience of their users, and to improve Samsung's position in the market.

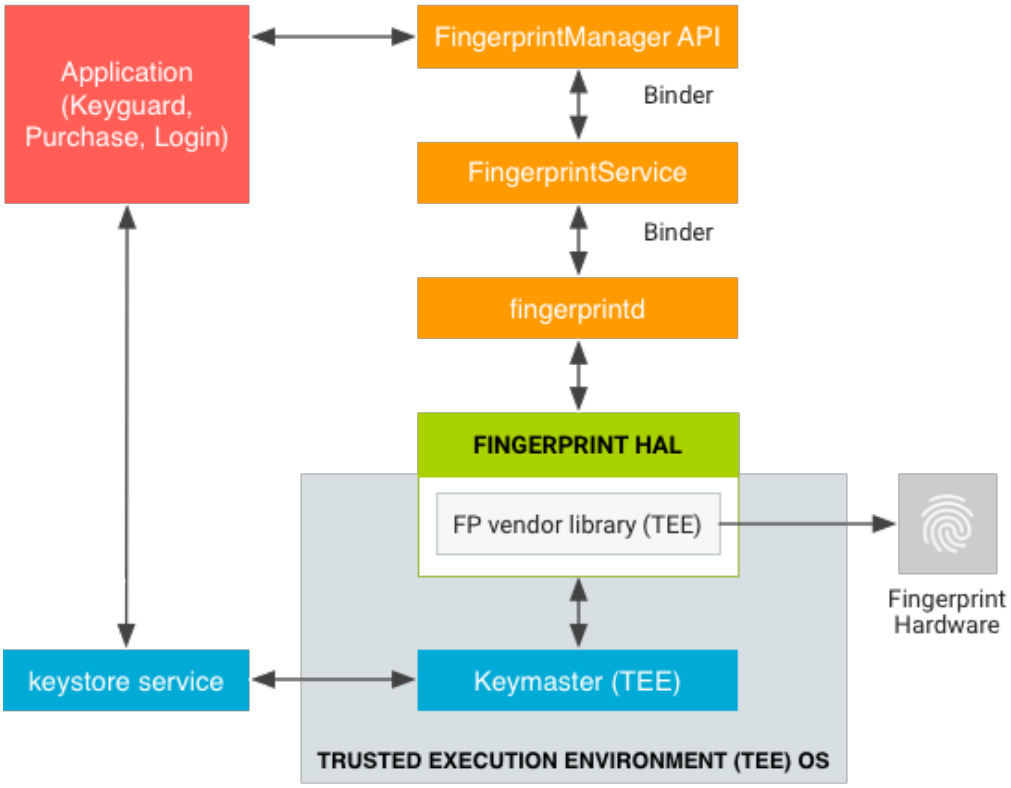
3. Samsung's Infringement of the Patents-in-Suit

41. Samsung Pay is described by Samsung as "an easy way to make purchases on your phone or watch." "It turns your device into a digital wallet that carries credit, debit, or gift cards." "And don't worry, you can use biometric security, so no one can access your financial data." Samsung advertises that "Samsung Pay is only available on select phone and watch models" and

that Samsung Pay may be used on a smart watch with a non-Samsung phone running Android 6.0 or later. **Exhibit 9 (Set up Samsung Pay on your phone, Samsung Support)**.

42. On information and belief, Samsung phones utilize Android's Fingerprint Hardware Interface Definition Language ("HIDL") to connect to its vendor-specific library and fingerprint hardware (e.g., a fingerprint sensor); to implement the Fingerprint HIDL, Samsung implements IBiometricsFingerprint.hal (the "Fingerprint HAL") in its vendor-specific library. Biometric data is protected because fingerprint templates must be signed with a private, device-specific key under the Fingerprint HIDL implemented by Samsung.

43. Fingerprint HAL interacts with Keystore Application Programming Interface ("API") and Keymaster components which provide hardware-backed cryptography for secure key storage in a secure environment, such as the Trusted Execution Environment ("TEE"). A high-level data flow for fingerprint authentication is produced below:

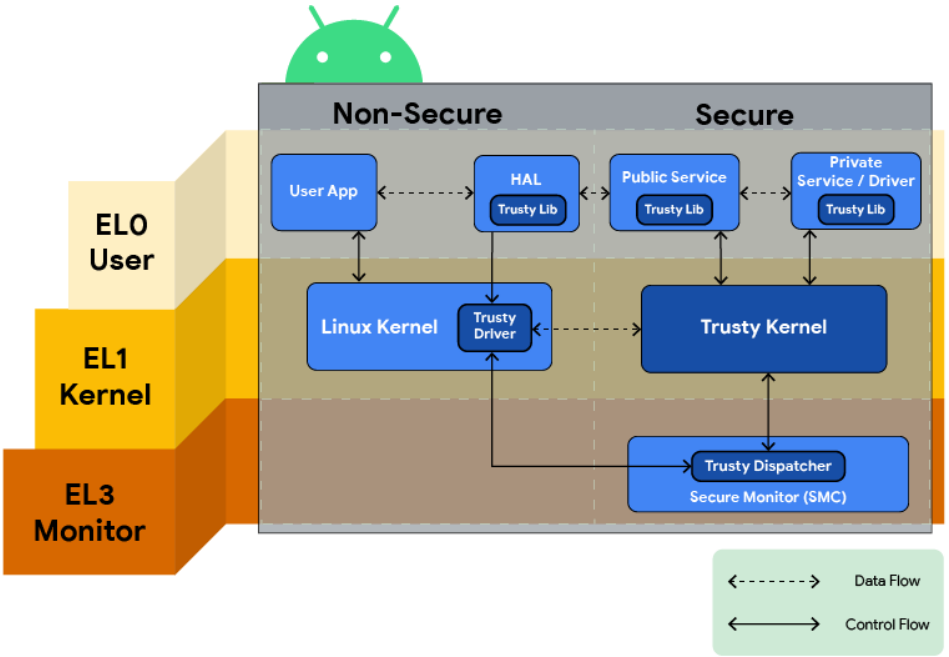


44. Keymaster functions include private key operations (*e.g.*, KeyPurpose:DECYPT and KeyPurpose::SIGN), e.g. a secret decryption value.

45. The Fingerprint HAL guidelines are described in the Android documentation as being designed to ensure that fingerprint data is not leaked and is removed when a user is removed from a device: Raw fingerprint data or derivatives (for example, templates) must never be accessible from outside the sensor driver or TEE. If the hardware supports a TEE, hardware access must be limited to the TEE and protected by an SELinux policy. The Serial Peripheral Interface (SPI) channel must be accessible only to the TEE and there must be an explicit SELinux policy on all device files. Fingerprint acquisition, enrollment, and recognition must occur inside the TEE.

46. "Trusty" is a secure Operating System ("OS") that provides a Trusted Execution Environment for Android, the operating system run on Samsung's smartphone devices. On information and belief, on Samsung's smartphone products, the Trusty OS runs on the same processor as the Android OS, and the two OS's run parallel to each other. Trusty has access to the full power of a device's main processor and memory but is completely isolated from the rest of the system by both hardware and software. Trusty's isolation protects it from malicious apps installed by the user and potential vulnerabilities that may be discovered in Android.

47. On ARM systems, like Samsung's devices, Trusty uses ARM's Trustzone™ to virtualize the main processor and create a secure TEE. An overview diagram of Trusty is reproduced below:



48. Uses for a TEE like Trusty include mobile payments, secure banking, multi-factor authentication, device reset protection, replay-protected persistent storage, and secure PIN and fingerprint processing.

49. Samsung describes that "[w]ith Samsung Pay, each transaction is covered by your bank's fraud protection and authenticated by your fingerprint, PIN or iris scan." "Plus, Samsung Knox and tokenization add extra layers of security." See **Exhibit 10 (Samsung Pay Website)**.

50. According to Samsung, Samsung Pay uses three levels of security to enable secure payments: fingerprint or iris-scanning authentication, tokenization and Samsung Knox, Samsung's defense-grade mobile security platform.

51. Samsung Knox "builds upon the Android Keystore by providing a tamper-proof, detection-based lock-down of cryptographic keys." On Samsung devices utilizing Knox, "the authentication software doesn't share or distribute the biometric measurements of any user." **Exhibit 11** (Knox Platform for Enterprise, Version 1.3.1 (2020)), page 41. "The measurements are stored in a format that can't be used to reproduce the original biometric, and can only be

accessed and decoded within the specific part of the TrustZone that has access to the biometric hardware." *Id*.

52. Visa has described Samsung Pay as "a simple way for customers to pay that meets all 2015 EMV security standards." *See* **Exhibit 12 (Visa and Samsung Pay)** . EMV, which originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard, is a payment method based upon a technical standard for smart payment cards and for payment terminals and automated teller machines which can accept them.

53. EMVCo, LLC ("EMVCo") facilitates worldwide interoperability and acceptance of secure payment transactions. EMVCo is supported by dozens of banks, merchants, processors, vendors and other industry stakeholders, including Samsung. EMVCo manages and evolves the EMV Specifications and related testing processes. This includes, but is not limited to, card and terminal evaluation, security evaluation, and management of interoperability issues. Samsung has received approval for the accused products as EMV Contactless Level 1 Mobile Products, *e.g.*, recently for the Samsung Galaxy S21 5G, Product Name SM-G991U. The publicly available approval letters, attached hereto as **Exhibit 13**, describe that EMVCo received a request for approval and found reasonable evidence that the submitted samples sufficiently conform to the EMV Contactless Interface Specification and other EMVCo requirements. Notably, EMV specifications were first published in 2007, years after the priority dates of all of the Patents-in-Suit.

54. One means of promoting payment security is "tokenization," an approach that substitutes sensitive data like account numbers and other personally identifiable information with a non-sensitive equivalent that has no intrinsic or exploitable meaning or value.

55. EMV payment tokens are open-loop tokens provisioned by a token service provider ("TSP"). Like other tokens, EMV payment tokens are used to replace the actual payment credential (*e.g.*, primary account number "PAN") with another numeric value.

56. The U.S. Payments Forum (formerly the EMV Migration Forum) is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of and enhance opportunities for payment transactions. According to the U.S. Payments Forum, Samsung was "among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases."

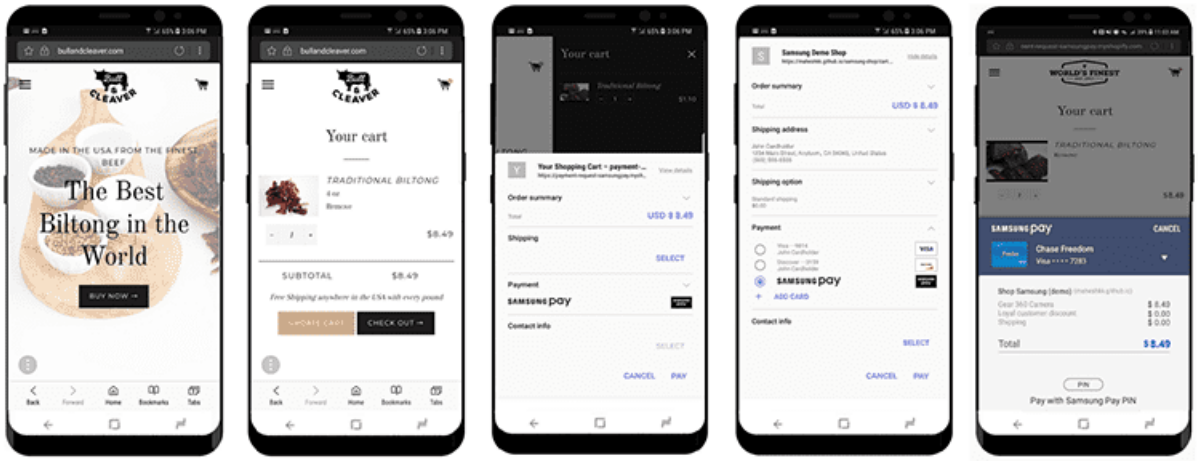
57. On information and belief, EMV payment tokens are issued to Samsung Pay equipped devices in exchange for a credit card number by a TSP such as Visa, Mastercard, American Express or Discover. On information and belief, device-specific payment tokens are stored by Samsung Pay-equipped devices.

58. The device-specific EMV payment tokens may be stored in three locations, one of them being a secure element / integrated circuit card ("ICC"). The first Samsung Pay-equipped devices, the Galaxy S6 and S6 Edge included a security cryptocontroller, *e.g.*, the Infineon SLE 97 ICC; on information and belief, subsequent devices equipped with Samsung Pay continued to use ICC elements. Secure elements like Infineon's SLE ICC are, according to the U.S. Payments Forum, "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

59. Samsung Pay requests biometric verification before providing payment credentials to merchants. The location/type of the purchase determines how the request is initiated.

60. For example, integrating the Samsung Pay API into their websites permits a merchant to accept Samsung Pay. When implemented via integration of the Samsung Pay API,

"the user initiates checkout, selects Samsung Pay as the preferred payment method, authenticates with a fingerprint or PIN, and voila — payment complete." Samsung further describes that "[w]hen properly implemented, the API also supports editing the billing/shipping address in Samsung Pay and selecting a different enrolled card before approving the transaction with a fingerprint scan or entering a PIN." See **Exhibit 14** (Samsung's Web Payments Integration Guide). A standard W3C implementation of Samsung Pay to a standard PaymentRequest object is shown below:



61. Samsung Pay also works with merchant apps on a user's smartphone. On information and belief, merchant apps installed on a user's smartphone communicate with Samsung Pay through the Samsung Pay API. A general use case takes the following form, according to Samsung:

62. To initiate payment, a merchant app calls the startIn-AppPay function of the API, which "initiates payment request with Samsung Pay." When the merchant app calls startIn-AppPay, Samsung Pay responds by presenting the user "with a payment sheet, which includes card selection and shipping address confirmation." After being presented the payment sheet, "the user then authenticates the payment method, amount, and delivery address with a fingerprint."

63. Samsung Pay also operates using NFC and/or MST: "Combining NFC with Samsung's proprietary MST technologies, Samsung Pay provides consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." *See* **Exhibit 15** (Samsung Pay Reaches One Year Anniversary in the United States, Samsung Newsroom (2016)). Samsung Pay equipped devices utilize the Android OS, as noted above. "Android 4.4 introduce[d] a new platform support for secure NFC-based transactions through Host Card Emulation (HCE), for

payments, loyalty programs, card access, transit passes, and other custom services." **Exhibit 16** (Android KitKat). When a user taps a phone to a payment terminal, "Android uses Application Identifiers (AIDs) as defined in ISO/IEC 7816-4 as the basis for routing transactions to the correct Android applications", such as the equipped Samsung Pay on Samsung's devices. When paying with Samsung Pay instore, "the app reads the transaction data and can use any local or network-based services to verify and then complete the transaction." *Id*. When opened in response to AID routing, Samsung Pay permits a user "to make a payment with [their] Favorite Cards, [by] swip[ing] up from the bottom of the screen. Then swip[ing] through and select[ing their] preferred card." *See* **Exhibit 17** (Make an in-store payment with Samsung Pay, Samsung Support). After selecting the card, the user "tap[s] PIN or IRIS . . . [or] simply place[s their] finger on [their] phone's fingerprint scanner". *Id.*.

64. Whether through AID routing, functions call between apps, or push notifications, regardless of where a user is shopping Samsung Pay equipped devices receive a request for biometric verification to authorize payment.

65. On Android devices like Samsung's devices, "the fingerprint sensor of [the] device is generally idle", but "in response to a call to authenticate . . . the fingerprint sensor listens for a touch". **Exhibit 18** (Android Open-Source Project: Fingerprint HIDL). After the user places their fingerprint on the sensor, a "vendor-specific library determines if there is a fingerprint match in the current set of enrolled fingerprint templates." *Id*.

66. Samsung Pay equipped devices wirelessly transmit EMV tokens to provide payment to merchants. When shopping online at a website, Samsung Pay equipped devices receive a push notification requesting authorization by the user, as detailed *supra*. "After user authenticates payment data is encrypted with partner's public key in user device, and will be sent

it to Samsung server" and made available to the merchant's website. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12.

67. The series of requests and responses permitting the merchant to receive payment, as summarized in Figure 10.1 of the EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020), begins with the merchant submitting a Token Payment Request for transaction routing. **Exhibit 20**. The data included within the Token Payment Request, as detailed in Table 10.1 of **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), is required to contain the payment token.

68. During transaction routing within the payment network, the Token Payment Request is transformed to a Token Authorization Request, as detailed in Figure 10.1 of **Exhibit 20**. As detailed in Table 10.3 of **Exhibit 20**, a required field of the Token Authorization Request generated by routing the Token Payment Request through payment network is a payment token. Accordingly, the payment token sent in the Token Payment Request from the merchant continues to persist during the token authorization request process. EMV payment tokens uniquely identifying Samsung Pay equipped devices and are provided during card enrollment, and thus are an identified embodiment of device ID codes specifically mentioned in at least the 730, 905, and 989 Patents.

69. "The Token Authorisation request process continues until De-Tokenisation has been completed." **Exhibit 20**, page 86. De-Tokenisation is performed by the token service provider. Visa, MasterCard, American Express and Discover each take on the role as TSPs. **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers). "Token Service Providers are responsible for a number of discrete

functions which may include, but are not limited to: Maintenance and operation of a Token Vault . . . [and] De-Tokenisation". **Exhibit 20** (EMV Payment Tokenisation Specification: Technical Framework, v2.2 (2020)), page 19.

70. Maintaining the token vault and providing de-tokenisation, token service providers keep a list of device ID codes uniquely identifying legitimate integrated devices. The token vault maintained by Visa, MasterCard, and other token service providers is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data". Maintaining the mapping between payment tokens and underlying primary account numbers, the token vault represents a list of legitimate tokens. EMV payment tokens, as detailed above, are values uniquely identifying Samsung Pay-equipped devices provided during card enrollment, and thus are an identified embodiment of device ID codes. As tokens are embodiments of device ID codes, the listing of legitimate payment tokens maintained by token service providers as part of the token vault is an identified embodiment of a list of device ID codes uniquely identifying legitimate integrated devices. TSPs are therefore one embodiment of a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices.

71. Opening the token vault to perform de-tokenisation occurs in response to receiving the token authorization request containing the payment token. De-Tokenisation is "the process of converting a Payment Token and Token Expiry Date to its underlying PAN and PAN Expiry Date based on the Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date stored in the Token Vault." **Exhibit 20** at 6. "The Payment Token SHALL be de-tokenised to the underlying PAN in the incoming Token Authorisation prior to sending the PAN Authorisation to the Card Issuer." *Id.*, at 91. Detokenizing in response to an incoming token

authorization requests requires the token service provider be sent the token authorization. As noted above, the token authorization sent to the TSP contains the payment token wirelessly sent from a Samsung Pay-equipped smartphone after successful biometric authentication. Authenticating a user via biometrics, as noted above, entails a vendor-specific library on the Samsung Pay-equipped devices comparing scan data from a sensor to biometric data to determine whether the scan data matches the biometric data.

72. When providing payment for in-app purchases, Samsung Pay equipped devices wirelessly transmit EMV tokens to merchants as payment. Specifically, "Encrypted payment information is passed from the Samsung Pay to the PG [(Payment Gateway)] through the merchant app". **Exhibit 21** (Samsung Pay Developers Onboarding and Project Integration Guide: In-App Payments for Merchants, Doc Rev 3.1-US (2017)), page 17.

73. In addition to providing payment information via virtual terminals, Samsung Pay equipped devices "combin[e] NFC with Samsung's proprietary MST technologies [to provide] consumers a way to pay almost anywhere you can swipe or tap a card at millions of merchant locations." Tapping a credit card is an example of contactless payment. "In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]) or NFC." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 39. By utilizing NFC, Samsung Pay-equipped devices can wirelessly transmit payment information to in-store terminals.

74. After the purchase has been authorized, Samsung Pay equipped devices "receive a push notification with details of [the] transaction after each purchase." **Exhibit 23** (View recent transactions in Samsung Pay). As the purchase can only be made after the primary account number

mapped to the token was released from the token vault and placed in an authorization request sent to the card issuer, the push notification received indicates allowed access to the file containing the account number. As shown in Figures 6, 7 and 11 of **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), this confirmation of access is either sent directly from the token service provider or indirectly from the token service provider as one of series messages flowing back to the Samsung Pay equipped smartphone.

75. Samsung Pay functionality is not limited to Samsung smartphone and tablet devices. Samsung's Galaxy Watch series also integrates with Samsung Pay. Samsung advertises that "you can use Samsung Pay on your watch!" An image that appears on Samsung's support page titled "Setting up your Samsung smart watch with or without your phone" is reproduced below:

76. The same support page describes that "[t]o access all its fun and useful features, you'll want to connect your smart watch to your phone using the Galaxy Wearable app.." **Exhibit 24**. As such, a Samsung smartphone or tablet with the Samsung Galaxy Wearable app (Wear

App) installed may act a personal digital key. Samsung smartphones and tablets communicate wirelessly, via an integrated receiver-decoder circuit enabling communication via Bluetooth, for example, with the Samsung Galaxy Watch, which also contains a receiver-decoder circuit external to the phone or tablet.

77. Samsung smartphone and tablets utilize a system on a chip (SoC) such as, in the case of its latest Galaxy S21 model, the Qualcomm Snapdragon 888 which provides several wireless interfaces including 5G, LTE, Bluetooth, and Wi-Fi. When communicating over a Bluetooth wireless connection, a proximity zone between the two devices is inherent, as the Bluetooth range may be approximately 30 feet.

78. The SoC interfaces with the various system components including the secure element, which is utilized to store, *inter alia*, secure biometric information for authenticating a user. The SoC must, like other system components, also interface with the battery of the smartphone or tablet.

79. On information and belief, Samsung's execution environment for Samsung Pay on its Galaxy Watch series includes an embedded secure element ("eSE"). Samsung has indicated such to EMVCo, as per the EMVCo Letter of Approval for the Galaxy Watch Active 2. eSE provides embedded, secure storage to "keep mobiles safe" by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." **Exhibit 25** (Samsung Security Solutions, Embedded security keeps mobiles safe).

80. The personal digital key component of Samsung's devices enable, *inter alia*, Samsung Pay.

81. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees have also complied with the marking provisions of 35 U.S.C. § 287.

CLAIM 1
(Infringement of the 730 Patent)

82. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

83. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 730 Patent.

84. Samsung infringes at least claims 1, 2, 5, 6, 8, and 9 of the 730 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

85. For example, Samsung directly infringes at least claim 1 and 5 of the 730 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States the software application Samsung Pay and products including Samsung Pay (*see* Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of the device.

86. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint and/or iris profile of a user, and codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value, in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered. Samsung devices utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example,

Samsung devices may utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

87. Samsung devices with Samsung Pay safeguard financial information, *e.g.*, credit card information, with EMV payment tokens as described *supra*. Indeed, Samsung was among the first to implement EMV payment tokens in digital wallets that hold credentials. On information and belief, the EMV payment tokens utilized by Samsung Pay uniquely identify the Samsung device. On further information and belief, the payment tokens are stored in a secure element that is tamper proof, *e.g.*, the Infineon SLE 97 ICC chip in the Galaxy S6 and S6 Edge. Secure elements are recognized as "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access."

88. Samsung devices with Samsung Pay also contain a secret decryption value, also called a "private key," which is used for, *inter alia*, decrypting, as specified in Android's keymaster functions, which provide hard-backed cryptography for secure key storage in a secure environment, such as the TEE, described *supra*. The secret decryption value, like the biometric data of the user and plurality of codes and other data values comprising a device idea, is tamper-proof as a result of being securely stored by the Samsung devices.

89. As described *supra*, Samsung devices with Samsung Pay may utilize biometric data, such as fingerprint and/or retina scan data from a biometric scan, and verify (*e.g.*, authenticate) biometric data of a user. The location of a purchase may determine how the request for verification is received (*e.g.*, a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores). When a Samsung device utilizes and verifies fingerprint biometric data,

for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

90. After receiving the determination that the scan data matches the biometric data, Samsung devices with Samsung Pay wirelessly send one or modes codes, including device ID codes, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens. EMV payment tokens, as detailed *supra*, are values uniquely identifying Samsung Pay preloaded smartphones provided during card enrollment, and thus are an identified embodiment of device ID codes. The payment tokens may be authenticated by an agent, *e.g.*, a token service provider.

91. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, e.g., token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token, which includes one or more codes from a plurality of codes and other data values including a device ID device, wirelessly transmitted by a Samsung device to the tokens stored in its repository for authenticated.

92. Samsung devices with Samsung Pay are further responsive to authentication by the agent, *e.g.*, token service providers, of the one or more codes and the other data values. For example, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. The push notification from the agent indicates that the user has been allowed access to an application, for example, an ATM machine, computer software, a web site and/or a file, *e.g.* which permits payment to occur.

93. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 730 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

94. Samsung also contributes to infringement by others of one or more claims of the 730 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 730 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

95. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 730 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 730 Patent.

96. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

97. Upon information and belief, Samsung will continue to infringe the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Samsung.

CLAIM 2
(Infringement of 905 Patent)

98. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

99. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 905 Patent.

100. Samsung infringes at least claims 1, 4, 5, 7, 9, 10, and 12 of the 905 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

101. For example, Samsung directly infringes at least claim 1 of the 905 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with Samsung Pay (see Appendix A). That software performs/executes, and those products provide, the method of claim 1, for example.

102. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or retina data, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) provided by Android which limits access to, and the ability to alter, biometric data.

103. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19** (EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (e.g., PAN) with another numeric value." *Id.*, at 8. Payment tokens, accordingly, are issued ("provisioned") to Samsung Pay preload smartphones in

exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id*., at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

104. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and iris-scanning, to verify a user. The location of a purchase may determine how the request for verification is received (*e.g*., a push notification received from a merchant's website, an API call from a merchant apps installed on the device, or direct prompt for Samsung Pay when using NFC (or MST) in stores).

105. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26** (Samsung Pay Web checkout Integration guide, Document version 1.4 (2018)), page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id*., at 6. Receiving a push notification prompting the user to authenticate by paying with their fingerprint, Samsung Pay preloaded smartphones therefore receive a request for biometric verification. Furthermore, Samsung devices with Samsung Pay receive scan data from a biometric scan carried out on a biometric sensor in response to receiving a request for biometric verification of a user.

106. When a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data from the fingerprint sensor of the device is compared with the existing fingerprint data on the device to determine whether there is a match.

107. After authenticating a user, Samsung devices with Samsung Pay wirelessly transmit one or modes codes, including device specific ID code, regardless of where the user is shopping. For example, Samsung devices wirelessly transmit EMV payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

108. Samsung devices with Samsung Pay are also responsive to an access message from agents that are a third-party trusted authority, *e.g.*, token service providers which are responsible for, *inter alia*, de-tokenization. These providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

109. After an ID code has been authenticated by a third-party trusted authority, Samsung devices with Samsung Pay "receive a push notification with details of [the] transaction after each purchase," *e.g.*, an access message. At this point, whereby the third-party trusted authority has confirmed that it successfully authenticated the token (*e.g.*, including the ID code), the user is allowed to complete a financial transaction.

110. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 905 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

111. Samsung also contributes to infringement by others of one or more claims of the 905 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly

infringe the 905 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

112. Samsung received actual and constructive notice of the 905 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 905 Patent.

113. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

114. Upon information and belief, Defendant will continue to infringe the 905 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 905 Patent by Defendant.

CLAIM 3
(Infringement of 989 Patent)

115. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

116. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 989 Patent.

117. Samsung infringes at least claims 1-6 of the 989 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

118. For example, Samsung directly infringes at least claim 1 of the 989 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay and products that are with

Samsung Pay (see Appendix A). That software performs/executes, and those products provide, a method for verifying a user during authentication of a device.

119. As described *supra*, Samsung devices are approved by EMVCo. "Samsung [was] among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases." **Exhibit 19**(EMV Payment Tokenization Primer and Lessons Learned, U.S. Payments Forum (2019)), page 12. "EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (*e.g.*, PAN) with another numeric value." *Id.*, p. 8. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. "[T]he TSP acts as a trusted service manager (TSM), delivering the token over the air or over an Internet connection to a device," *e.g.*, Samsung devices with Samsung Pay. *Id.*, p. 12. "As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor." *Id.*, at page 16. This token, received by the Samsung devices, therefore contains an ID code that uniquely identifies the smartphone among a plurality of smartphones.

120. As described *supra*, Samsung devices with Samsung Pay persistently store biometric user data, *e.g.*, a fingerprint or iris profile of a user, and an ID code, *e.g.*, a device-specific code that uniquely identifies a specific Samsung device. Samsung devices further utilize Samsung Knox and "the authentication software doesn't share or distribute the biometric measurements of any user." For example, Samsung devices utilize Fingerprint Hardware Interface Definition Language (HIDL) which limits access to, and the ability to alter, biometric data.

121. As for the device specific code, on information and belief, payment tokens are unique for each device, as required by EMV. Payment tokens are issued ("provisioned") to

Samsung devices with Samsung Pay in exchange for a credit card number by a token service provider (TSP), such as Visa, MasterCard, Discover, and American Express. *Id*., at 23 (Figure 5 – identifying Visa, MasterCard, American Express and Discover as Token Service Providers).

122. As described *supra*, Samsung devices with Samsung Pay may receive biometric data, such as fingerprint and retina data, and authenticate such biometric data. The location of the purchase determines the type of verification carried out (*e.g*., a merchant's website, merchant apps installed on the device, or use of NFC (or MST) that provides a "way to pay almost anywhere you can swipe or tap a card at millions of merchant locations."

123. For example, on a Samsung Pay equipped website, a "user can select 'Samsung pay' option to pay, and then payment requesting push message will [] arrive[] to [a] user's device and the payment can be confirmed by user authentication." **Exhibit 26**, page 7. When the user clicks on the push notification received on their Samsung Pay preload smartphone, a "Payment Sheet is opened [and] User authentication is performed" giving the user the option to "pay with fingerprint". *Id*., at 6. As part of the authentication, Samsung devices with Samsung Pay receive scan data from a biometric scan using the smartphone.

124. Where a Samsung device utilizes and authenticates fingerprint biometric data, for example, scan data is compared with the fingerprint data on the device to determine whether there is a match.

125. After authenticating a user (*e.g*., making a determination that the scan data matches the biometric data), a Samsung device with Samsung Pay wirelessly sends one or modes codes, including device specific ID code, regardless of where the user is shopping, to a third-party trusted authority, *e.g*., token service providers. For example, Samsung devices wirelessly transmit EMV

payment tokens which contain codes uniquely identifying the Samsung Pay device provided during card enrollment.

126. Token service providers also maintain a token vault, which is a "repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data." The providers compare the token wirelessly transmitted by the Samsung device to the tokens stored in its repository, which include previously registered ID codes.

127. In response to a purchase having been authorized (e.g., after successful comparison of the token sent by the Samsung device to the token(s) stored in the repository) by the provider, the transaction is completed and the Samsung device "receive[s] a push notification with details of [the] transaction after each purchase." The transaction includes either access to an ATM machine or a financial account (e.g., a credit card).

128. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 989 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

129. Samsung also contributes to infringement by others of one or more claims of the 989 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 989 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

130. Samsung received constructive notice of the 730 Patent at least as early as July 2017 and actual notice of the 989 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement,

with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 989 Patent.

131. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 989 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

132. Upon information and belief, Defendant will continue to infringe the 989 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 989 Patent by Defendant.

CLAIM 4
(Infringement of 188 Patent)

133. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

134. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 188 Patent.

135. Samsung infringes at least claims 1, 3-10, and 13-16 of the 188 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

136. For example, Samsung directly infringes at least claims 1 and 10 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 10 and those products provide the hybrid device of claim 1, for example.

137. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured biometric information.

138. The key utilized by the Wear App to control access to the memory of the Android smartphone by a paired Galaxy Watch may take on various forms. The key may be a cryptographic key such that an "encryption engine 254 encrypts/decrypts data 228 flowing to/from the service block 112 based on the access key 118 (or some other key generated based on the access key, for example a session key)". 188 Patent, Col. 6, ll. 33-37. In lieu of cryptology, the key may uniquely identify the paired Galaxy Watch. In such instances, the key may be "a PDK ID 212 [] used as an identifying feature of a PDK 102 and distinguish[ing] between PDKs 102 in private or Central registry entries". *Id*., Col. 5, ll. 66 to Col. 6, ll. 2. Besides a unique identifier or crypto-key, the key used by the Wear App to control memory access by a paired Galaxy Watch may be a "basic authentication function that allows the PDK and sensor to verify each other. In this scenario, once the sensor and PDK finish their verification the application is signaled". *Id*., Col. 9, ll. 28-31 ("[T]he RDC 304a represents and includes the functionality described above as being provided by the sensor 108." Id, Col. 13, ll. 58-60.).

139. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access keys to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control

access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id*. By pairing a Galaxy Watch with the Samsung device, the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

140. Samsung devices, including those with the Samsung Galaxy Wearable app, store local, secured biometric information as per Android's implementation guidelines which require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". Exhibit R (Android Open-Source Project: Fingerprint HIDL). Per these guidelines, biometric information, *e.g.*, fingerprint data never leaves the TEE. Furthermore, Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted exaction environment" isolated from the rest of the system. **Exhibit 28** (Android Open-Source Project: Trusty TEE). Accordingly, biometric information, *e.g.*, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing, Trusty.

141. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, e.g. Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy

Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

142. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, inter alia, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—e.g., a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

143. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". Id. Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

144. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13,

EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Exhibit 25 (Embedded security keeps mobiles safe). Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

145. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

146. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, inter alia, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

147. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 188 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

148. Samsung also contributes to infringement by others of one or more claims of the 188 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

149. Samsung received actual and constructive notice of the 188 Patent on or around July 2017. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 188 Patent.

150. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 188 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

151. Upon information and belief, Defendant will continue to infringe the 188 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

CLAIM 5
(Infringement of 700 Patent)

152. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

153. Proxense has not licensed or otherwise authorized Samsung to make, use, offer for sale, sell, or important any products that embody the inventions of the 700 Patent.

154. Samsung infringes at least claims 1, 3, 5-9, 11, 15-17 and 19 of the 700 Patent in violation of 35 U.S.C. § 271 with respect to Samsung Pay with the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

155. For example, Samsung directly infringes at least claims 1 and 11 of the 188 Patent by making, using (*e.g.*, performing/executing), selling, and/or offering to sell within the United States software applications including, but not limited to, Samsung Pay, the Samsung Galaxy Wearable App and/or products that are with Samsung Pay (see Appendix A). Samsung Pay and/or the Samsung Galaxy Wearable App performs/executes the method of claim 11 and those products provide the hybrid device of claim 1, for example.

156. As described *supra*, Samsung devices with the Samsung Galaxy Wearable app enables applications on a paired Galaxy Watch to access memory on the smartphone or tablet, which stores local, secured financial information.

157. Whether a crypto-key, unique identifier, or basic authentication, the Wear App functions as a controller by utilizing access secured financial information (*e.g.*, keys) to control access to the smartphone's memory. Pairing a Galaxy Watch to an Android 6.0 and higher smartphone via Bluetooth, the Wear App acting as a controller has access to each of these types of keys. "When a device is paired, the basic information about the device – such as the device's name, class and MAC address – is saved". **Exhibit 27** (Bluetooth Overview, Android Developers). Pairing a Galaxy Watch with an Android smartphone, accordingly, provides various identification keys usable by the Wear App to control access to memory. Additionally, "to be *paired* means that two devices … have a shared link-key that can be used for authentication, and are capable of establishing an encrypted connection". *Id*. By pairing a Galaxy Watch with the Samsung device,

the Wear App also gains access to authentication keys and crypto keys, which may be used to control access to the phone's memory. Samsung devices with the Samsung Galaxy Wearable app therefore comprise a personal digital key.

158. The integrated personal digital key of the Samsung devices with the Samsung Galaxy Wearable app is also capable of communicating wireless with an external receiver-decoder circuit. For example, using Bluetooth, which is provided through SoCs integrated into Samsung devices, *e.g*. Qualcomm's Snapdragon, the personal digital key may communicate with a Samsung Galaxy Watch. As detailed by Samsung, "Install the Galaxy Wearable application on your mobile device, then pair your wearable devices via Bluetooth to enjoy all of its features." Galaxy Wearable, App on Google Play. Pairing a device and a watch with the Samsung Galaxy Wearable app via Bluetooth further requires the paired Samsung Galaxy Watch to have an external receiver decoder circuit to the smartphone. A Samsung device with the Wear App, therefore, contains an "integrated personal digital key (PDK) … capable of communicating wirelessly with an external receiver-decoder circuit (RDC)".

159. As described above, the Samsung devices include a SoC with a receiver decoder circuit which provides, *inter alia*, Bluetooth capability. The receiver decoder circuit communicates wireless (*e.g.*, via Bluetooth) with an external personal digital key—*e.g.*, a Samsung Galaxy Watch. With their own counterpart to the Wear App to enable pairing over a Bluetooth, as well as an embedded secure element (eSE) storing payment information, Samsung Galaxy Watches constitute personal digital keys.

160. In addition to a Bluetooth transceiver communicating with an RDC, Samsung Galaxy Smart watches have an eSE storing information particular to a user. One feature enabled by pairing a Samsung Galaxy Watch to an Android 6.0 and higher smartphone is the ability to use

Samsung Pay on the paired Galaxy Watch. Adding a credit card to Samsung Pay on a Galaxy watch requires, "[o]n your phone, open[ing] the Galaxy Wearable app… then tap[ping] Add credit or debit card." **Exhibit 29** (Add a payment card to Samsung Pay). The user may then "take a photo of the card number or manually enter them". *Id*. Regardless of how entered, the card information must get from the phone to the Galaxy Watch, most likely as a EMV Payment Token received on the phone in response to a request by Samsung Pay to a Token Service Provider (TSP), and then be stored on the Galaxy Watch.

161. Samsung identifies the execution environment of Samsung Pay on, for example, the Samsung Galaxy Watch Active 2 as including an eSE (embedded secure element). Exhibit 13, EMVCo Letter of Approval – EMV Contactless Level 1 Mobile Product, Approval No. MTA_LOA_SAEL_02082, page 2 (identifying the "execution environment" as including an "eSE"). Samsung describes that its eSE provides secure storage by "generating an unclonable key and a security-enhanced processing unit, Samsung eSE secures sensitive data and protects against digital attack." Embedded security keeps mobiles safe, http://www.samsung.com/semiconductor/security/ese/. Credit card information (EMV Payment Token) received from the Samsung smartphone or tablet is therefore stored in the eSE on the watch. A Galaxy Watch paired to the PDK provided on Samsung smartphone or tablet by the Wear App, therefore contains memory storing information particular to a user.

162. The integrated receiver decoder circuit of the smartphone or tablet, e.g. the SoC, is coupled to the personal digital key by a first signal line. As described *supra*, a Samsung device with the Samsung Galaxy Wearable app requires "storage" permission "used to transmit and receive stored files" with a Samsung Galaxy Watch and therefore a first signal line is used to

transmit files from storage to the SoC. The integrated receiver decoder circuit is also coupled to, *inter alia*, the device's battery.

163. Ultimately, the personal digital key of a Samsung device with the Samsung Galaxy Wearable app may enable, *inter alia*, Samsung Pay. "Instal[ing] the Galaxy Wearable application on your mobile device, then pair[ing] your wearable devices via Bluetooth [allows you] to enjoy all of its features." Galaxy Wearable, App on Google Play. "Before you can use Samsung Pay on your watch, you need to connect your watch to your phone". Exhibit 29 (Add a payment card to Samsung Pay). "After initial setup, Samsung Pay on Galaxy Watch can make at least five transactions without reconnecting to a network… via Bluetooth pairing with compatible smartphone." Exhibit 30 (Samsung Galaxy Watch – Our Newest Smartwatch, Samsung US).

164. Samsung has induced infringement, and continues to induce infringement, of one or more claims of the 700 Patent under 35 U.S.C. § 271(b), by sellers, resellers and end-user customers who use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

165. Samsung also contributes to infringement by others of one or more claims of the 700 Patent under 35 U.S.C. § 271(c), such as sellers, resellers and end-user customers who directly infringe the 188 Patent when they use, make, accept, and/or process payments made using Samsung Pay via the Accused Products.

166. Samsung received constructive notice of the 700 Patent at least as early as July 2017 and actual notice of the 700 Patent at least as early as the filing of this Complaint. Samsung performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 700 Patent.

167. Proxense has been injured and seeks damages to adequately compensate it for Samsung's infringement of the 700 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

168. Upon information and belief, Defendant will continue to infringe the 700 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 188 Patent by Defendant.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants infringe one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendants' infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendants' infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: March 5, 2021

Respectfully submitted,

/s/ Erick S. Robinson

David L. Hecht (PHV to be submitted) (**lead counsel**)
Maxim Price (PHV to be submitted)
Conor B. McDonough (PHV to be submitted)
Yi Wen Wu (PHV to be submitted)
James Zak (PHV to be submitted)
dhecht@hechtpartners.com
mprice@hechtpartners.com
cmcdonough@hechtpartners.com
wwu@hechtpartners.com
jzak@hechtpartners.com
HECHT PARTNERS LLP
125 Park Avenue, 25th Floor
New York, NY 10017
P: (212) 851-6821
dhecht@hechtpartners.com

-and-

Erick S. Robinson
Texas Bar No. 24039142
erobinson@porterhedges.com
PORTER HEDGES LLP
1000 Main Street, 36th Floor
Houston, Texas 77002
P (713) 226-6615
F: (713) 226-6215

ATTORNEYS FOR PLAINTIFF
Proxense, LLC

EXHIBIT 16

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC, *Plaintiffs*, v. GOOGLE LLC and GOOGLE PAYMENT CORP. *Defendants*.	Civil Action No. 6:23-cv-320 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendants Google LLC and Google Payment Corp. ("Google" or "Defendant"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Google infringes one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. On information and belief, Google LLC is a Delaware corporation with a physical address of 500 West Second Street, Austin, Texas, 78601. On information and belief, Google LLC

also maintains a regular and established place of business at 110 East Houston Street, #300, San Antonio, Texas 78205. Google LLC is registered to do business in the State of Texas and has been registered since 2006. Google LLC may be served through its registered agent, the Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, at 211 East Seventh Street, Suite 620, Austin, Texas, 78701 - 3218.

4. Google Payment Corp. is a Delaware corporation and maintains its principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google Payment Corp. is registered to do business in the State of Texas and has been registered since 2005. Google Payment Corp. may be served with process through its registered agent, Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, at 211 East Seventh Street, Suite 620, Austin, Texas, 78701 - 3218.

JURISDICTION AND VENUE

5. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

6. This Court has personal jurisdiction over Google LLC and Google Payment Corp. (collectively, "Google") because Google is a multinational technology company that has a significant presence in the District through the products and services Google provides residents of this District. Defendants regularly conduct business and have committed acts of patent infringement within this Judicial District that give rise to this action and have established minimum contacts within this forum such that the exercise of jurisdiction over Google would not offend traditional notions of fair play and substantial justice. Google has committed and continues to

commit acts of infringement in this Judicial District, by, among other things, offering to sell, selling, using, importing, and/or making products and services that infringe the asserted patents. Google has further induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

7. On information and belief, Google has authorized retailers in this Judicial District that offer and sell products on its behalf in this District, including products accused of infringement herein. On information and belief, these include Best Buy, *e.g.*, at 4627 S. Jack Kultgen Expy., Waco, TX 76706; Target, e.g., at 5401 Bosque Blvd., Waco, TX 76710; T-Mobile, *e.g.*, 100 N New Rd Ste 110, Waco, TX 76710 and 2448 West Loop 340 Suite 24a, TX 76711; and Verizon, *e.g.*, 1820 S Valley Mills Dr., Waco, TX 76711 and 2812 W Loop 340 Waco, TX, 76711.

8. Proxense's causes of action arise directly from Google's business contacts and other activities in the State of Texas and this District.

9. Google has derived substantial revenues from its infringing acts within the State of Texas and this District.

10. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1400(b). Google is registered to do business in Texas and, upon information and belief, Google has transacted business in the Western District of Texas and has a regular and established places of business in this Judicial District.

11. Joinder of Google LLC and Google Payment Corp. is proper because they are related entities that are either jointly and severally liable for infringement, or that make, use, sell, offer to sell, and/or import the same or similar products accused of infringement herein. Further, upon information and belief, Google LLC and Google Payment Corp. act in concert to provide the

software, hardware, infrastructure, and payment networks used by the accused products. Therefore, the factual question of infringement will substantially overlap between Google LLC and Google Payment Corp. Additionally, Proxense anticipates there will be substantial overlap with respect to discovery.

12. Google also maintains a significant physical presence in this Judicial District and employs many people in this Judicial District. According to CultureMap Austin, Google already leases more than 550,000 square feet at three locations in and around downtown Austin: 100 Congress Ave., 901 E. Fifth St., and 500 W. Second St. *See* John Egan, "Austin's next iconic high-rise sails towards opening date with Google as anchor tenant," CultureMap Austin (March 19, 2021) *See* **Exhibit 7** In addition to its current offices, including its Austin headquarters at 500 W 2nd Street in Austin, Google has leased an entire building down the street at 601 West 2nd Street that is being built out. Last year, Google announced that it plans to occupy the 37-story building, which will be Austin's tallest office tower and contains 814,081 square feet. *Id*.

13. Google currently employs approximately 1,100 people in Austin. Among these employees are people specifically responsible for the infringing technology in this lawsuit. For example, Nik Bhattacharya, a Senior Software Engineering Manager, who works for Google in Austin, Texas, describes on his LinkedIn profile that he is "**[l]eading** the FIDO passkeys effort at Google." *See* **Exhibit 8**. Aspects of Google's particular implementation of FIDO are among the grounds for the claims of patent infringement asserted here.

14. On Google's Careers website, careers.google.com, as of December 15, 2022, Google lists 209 open jobs for its Austin, Texas location. Many of its jobs list multiple potential locations for the job applicant to work from, because Google employees are able to work collaboratively from essentially anywhere, on the "cloud," because all relevant information,

including on information and belief documents relevant to this litigation, including documents and code are decentralized and exist on Google's intranet that is available from any of its physical office locations, or even remotely. By way of a non-limiting example, as of December 15, 2022, Google's Careers website had a listing for a Senior Product Manager, Core Privacy, Safety, and Security. The position listed potential in-office locations as Seattle, Washington; Austin, Texas; and New York City, New York. The position's responsibilities included: "[l]aunch[ing] new products and features…"; "[w]ork[ing] collaboratively with engineering, marketing, legal, UX, and other teams on cutting edge technologies"; and "[d]evelop[ing] solutions to problems by collaborating as needed across regions, product areas, and functions."

15. On information and belief, Google has also committed acts of direct and indirect infringement in the Western District of Texas. For example, Google sells its Pixel line of phones to individuals in this Judicial District, which ship with various versions of the Android operating system ("Android OS" or "Android"). Google also distributes Google Pay, also known as "G Pay," "Pay with Google" and "Android Pay" which it describes as a "simple, secure way to pay and save," in this Judicial District, both on its Pixel phones and otherwise. *See* **Exhibit 9**.

PATENTS-IN-SUIT

16. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 1**.

17. On November 11, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,886,954 (the "954 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 954 Patent is attached hereto as **Exhibit 2**.

18. On March 26, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,298,905 (the "905 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 905 Patent is attached hereto as **Exhibit 3**.

19. On February 4, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,646,042 (the "042 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 042 Patent is attached hereto as **Exhibit 4**.

20. On June 13, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,679,289 (the "289 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 289 Patent is attached hereto as **Exhibit 5**.

21. On September 11, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,073,960 (the "960 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 960 Patent is attached hereto as **Exhibit 6**.

22. Proxense is the sole and exclusive owner of all right, title, and interest to and in, or is the exclusive licensee with the right to sue for, the 730, 954, 905, 042, 289, and 960 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

23. The technologies of the Patents-in-Suit were invented by John Giobbi. The 730 and 905 Patents generally cover systems and methods for an integrated device that persistently

stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (e.g., a fingerprint) can be compared against the stored biometric data. Once the user has been biometrically verified by the integrated device, a code can be wirelessly transmitted for authentication. The 042, 289, and 960 Patents generally covers systems, devices, and methods of utilizing personal digital keys for verifying a user in order to enable applications, functions, or services.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

24. Authentication is the process by which the identity of a user is confirmed on a device, including computers, tablets, and phones. When a person is authenticated, the goal is to verify that the credentials presented are authentic. For years, users were authenticated with usernames and passwords. However, with the amount of sensitive personal and financial information currently stored on personal devices, and the rise of biometric readers and high-speed networks, there was a need to implement improved authentication architectures.

25. One such architecture is "federated authentication" (also known as "federated identity"), which relies on an external trusted system to authenticate users. In a federated authentication solution, the system being accessed must request authentication of the user from the external system that is used to authenticate users. The external system authenticating the user will then communicate successful authentication back to the system being accessed. Successful authentication is communicated between the two systems with the issuance security tokens containing claims about user authentication. Upon successful authentication of a user, the external system issues a security token which can be exchanged for access to the other system. One such federated architecture is OpenID Connect.

26. While OpenID connect limited the use of passwords, it did not eliminate them. Authentication protocols geared towards eliminating passwords include WebAuthn and its derivative, FIDO2, an open authentication standard developed by the FIDO alliance. WebAuthn, and the derivative protocol FIDO2, utilize an asymmetric key pair to authenticate a device. Possession and control of the device verifies the identity of the user. The device, referred to as an authenticator, generates a private/public key pair and a credential ID uniquely identifying the key pair. The public key and credential ID are sent to the authentication server – called in the protocol the "relying party". The private key is held by the authenticator. During authentication, the authenticator sends a signature generated with its private key and the credential ID identifying the private key used to generate the signature. The relying party (i.e., authentication server) uses the credential ID to retrieve the matching public key. The signature is then verified with the public key. Upon successful verification of the signature, the relying party issues an authentication response.

27. WebAuthn and federated protocols can be combined. When combined, the system to be accessed by the user requests authentication by a WebAuthn / FIDO 2 server. The server issues an authentication request to the user's authenticator. The authenticator responds by providing a signature and credential ID to the WebAuthn/FIDO2 server. If the signature is verified, the WebAuthn/FIDO2 server informs the OpenID connect of successful authentication. The OpenID connect server then sends a security token to be used to access the system requesting authentication.

28. Attempting to eliminate the user of passwords, Google has developed a universal platform "passwordless" architecture. The architecture is universal in that it works across platforms, such as iOS, Android, and Windows. It is password-less in that passwords have been

replaced with the use of authenticators incorporated into Android OS 9 and higher. Incorporating OpenID Connect, Google's architecture relies on the issuance of security tokens. The hub of Google's universal platform password-less architecture is Google Identity, which receives authentication requests from external systems, coordinates the action of authenticators, and issues security tokens.

29. Federated authentication is not the only authentication architecture Google has incorporated into the Android OS. Google has incorporated EMV's payment tokenization architecture. As with OpenID Connect, EMV's payment tokenization utilizes token issued by a third-party and stored on the phone. The tokens are a surrogate for a credit card, debit card, or other Primary Account Number (PAN), and can be used anywhere the underlying account is accepted as payment. As with OpenID Connect tokens, EMV payment tokens indicate a previous authentication of the user. The tokens differ with respect to authorization claims. OpenID authenticates the user and obtains the user's consent before issuing a token. As such, the token represents authentication of the user and what the user has been authorized. As authorization is obtained before token issuance, a token can never be used for more than authorization claim it contains. EMV tokens, on the other hand, contain no claims with respect to authorization. Authorization, rather, is indicated by release of payment from a device. Unlike OpenID Connect tokens, payment tokens are locked in a device and can only be released following verification of the user by the device. As only the legitimate use can be verified, release of an EMV token is indicative of user consent. Presentation of an EMV payment token, accordingly, is indicative of user consent to the accompany charge to their account. Regardless of the differences in their manner of representing authorization and the timing of obtaining authorization, both OpenID connect tokens and EMV tokens are indicative of user authentication and authorization.

30. As to facilitate the use of EMV's payment tokenization architecture, Google has deployed technology to secure payment tokens in connection with its Android OS, Google Pay (initially and subsequently called Google Wallet, collectively "Google Pay" unless otherwise specified). Using biometric security features (i.e., the ability to unlock mobile devices through a fingerprint or facial recognition) available in Android, Google offered biometric authentication of the Google Pay app, in 2019. *See* **Exhibit 10**. Previously, the only Google Pay authentication option was entering a PIN number, which is guessable and "crackable," as opposed to more secure and user-friendly biometrics.

31. Incorporating authenticators (including Google's Authenticator) into the Android OS is, on information and belief, necessary for Google Cloud Services to remain competitive with Microsoft's cloud services, which supports the Windows 10/11 integrated authenticator, Windows Hello, and the iOS/Android authenticator, Microsoft Authenticator. The worldwide public cloud services market had revenues in 2021 totaling $408.6 billion. Likewise, the ability to secure Google Pay transactions with biometrics was, on information and belief, important for Google to remain competitive with Apple Pay and other payment platforms that had implemented the feature. Global contactless transaction values were estimated at $2 trillion in 2020. By 2024, they may reach $6 trillion according to forecasts. Mobile payments, or transactions initiated on mobile devices such as cell phones or tablet computers, have become increasingly popular with the increasing use of applications like Google Pay (also known as Google Wallet), launched in 2011.

II. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

32. Proxense was founded in 2001.[1] From approximately 2004-2012, Proxense developed, *inter alia*, mobile payment technologies and commercial products, employing over thirty engineers, and investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

33. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

34. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including the asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed

[1] The company was formally incorporated as an LLC in 2001 under the name Margent Development LLC; in 2005, the business was renamed to Proxense LLC.

over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

35. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 11**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), *See* **Exhibit 12**.

36. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), *See* **Exhibit 13**. The DARKReading article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

37. It would be years until products like Google Wallet (2011), Apple Pay (2014), and Samsung Pay (2015) were launched and became mainstream; Apple's TouchID, which involves fingerprint recognition technology, for example, was introduced in 2013. It would take Google

until 2019 to enable biometric authentication for Android 10 phones and Google Pay. Accordingly, Proxense's technology was years ahead of the industry.

38. After the launch of services like Google Wallet/Pay, and its inextricable link to the some of the most popular smartphone hardware devices in the United States, and the world, Proxense would find itself unable to compete with companies like Google, even though Proxense invented the technology utilized in these solutions.

39. Today, Proxense holds 80 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management and mobile payments. Proxense continues to prosecute new patents on its proprietary technology.

III. INFRINGEMENT ALLEGATIONS

1. The Accused Products

40. Through its own actions, and the actions of its customers and users, which Google directs and controls, Google has manufactured, used, marketed, sold, offered for sale, and exported from and imported into the United States a universal platform password-less architecture that directly and/or indirectly infringes (and literally or via the doctrine of equivalents) the Patents-in-Suit. Accordingly, the Accused Products include the servers, cloud resources, and software comprising Google's password-less architecture and devices including, supporting and integrating into the architecture, including devices running the Android OS, Chrome OS, and/or Chrome browser.

41. Three primary components make up the infringing identity architecture. The first is Google Identity (also known as Google Identity Services) which coordinates the actions of the other components by authenticating users and issuing various bearer tokens. See e.g., **Exhibit 14**. The second is an authenticator, like Google Authenticator, permitting user verification by Google

Identity. During verification, Google Identity issues commands to the authenticators (called "requests"). The operation of the authenticators, accordingly, is controlled by Google. The third component of the system is a resource, such as an application, website, or subscription, requesting authentication of the user. During user login, the resource sends requests to a URL provided by Google and in a form dictated by Google. The resource then listens for a reply at a callback URL the resource registered with Google. As with the requests, the callbacks are in the form dictated by Google. The resources are hosted by device and/or server separate from Google Identity. Accordingly, the resource and Google Identity are separate and distinct entities and the resource (not Google Identity) is the system being accessed.

42. Google utilizes Google Identity to sign users into Gmail, Google Drive, Google Pay and other services and products offered by Google. Google sells access to Google Identity to developers, websites, and corporate clients through various subscriptions. Thus, for a fee, Google Identity becomes an identity provider for applications, businesses, and websites. Selling such identity and access management (IAM) services and controlling the actions of subscribers and users, Google directly and/or indirectly infringes (and literally or under the doctrine of equivalents) the Patents-in-Suit. Furthermore, by utilizing Google Platform for its own product and services, Google directly and/or indirectly infringes (and literally or via the doctrine of equivalents) the Patents-in-Suit.

43. As noted above, Google's infringing universal platform password-less architecture includes an authenticator. One authenticator distributed by Google is a native component of Android OS 9 and higher. Accordingly, since at least August 6, 2018, if not earlier, the Android OS has enabled password-less sign-in to services and subscriptions offered by Google. *See* **Exhibit 15**. Another authenticator developed by Google is the Titan Security Key that includes

the functionality to wirelessly verify a user during authentication of an iOS compatible devices. **Exhibit 16**. The current and previous versions of the Android OS and Titan Security Key are non-limiting instances of authenticators integrated into the Accused Products.

44. Google Identity, which directs and controls the actions of the authenticator, is also an element of the Accused Products. Google Identity includes a series of APIs launched on August 3, 2021. *See* Google Developers Blog: Launching our new Google Identity Services APIs (googleblog.com), August 3, 2021, **Exhibit 17** ("Today we are launching our new family of Identity APIs called Google Identity Services."). Google operates and maintains Google Identity. When combined with authenticators, such the Android OS and Titan Security Key, consumers of Google's products and services receive the benefit of password-less biometric authentication across platforms. For instance, a user may log into and utilize Gmail or Google Pay on their Windows PC or iOS device. Third party developers can purchase identity and access management services from Google to integrate their applications with Google Identity in order to offer cross platform password-less authentication via biometrics and the use of ID and access tokens to their customers and subscribers. Developers subscribing to Google Identity must register their application or website with Google, request authentication by sending a request to a URL provided by Google and in a format dictated by Google, and listen for a callback provided by Google that contains a message generated by Google in a format controlled by Google.

45. The Accused Products also include a resource accessed following successful authentication of the authenticator by Google Identity. As noted above, the resource may be an application, website, and/or a subscription offered by Google, a subscribing business, or a subscribing developer. When a user has been authenticated via an authenticator offered by Google, various bearer tokens are returned by Google to the callback URL registered with Google Identity.

The bearer token allows access to the application, and as such is an access message. Regardless of whether the resource is an application, a subscription, or a service offered by Google or a subscribing developer or business, the resource is on a system separate and distinct from Google Identity. Distribution of bearer tokens and other such access messages by Google Identity is thus necessary for Google Identity to inform the resource that the user has been successfully authenticated via an authenticator distributed by Google. As the bearer tokens are generated and distributed by Google Identity, Google controls their form and how they are distributed.

46. Current and previous versions of Google Identity are non-limiting instances of the Accused Products.

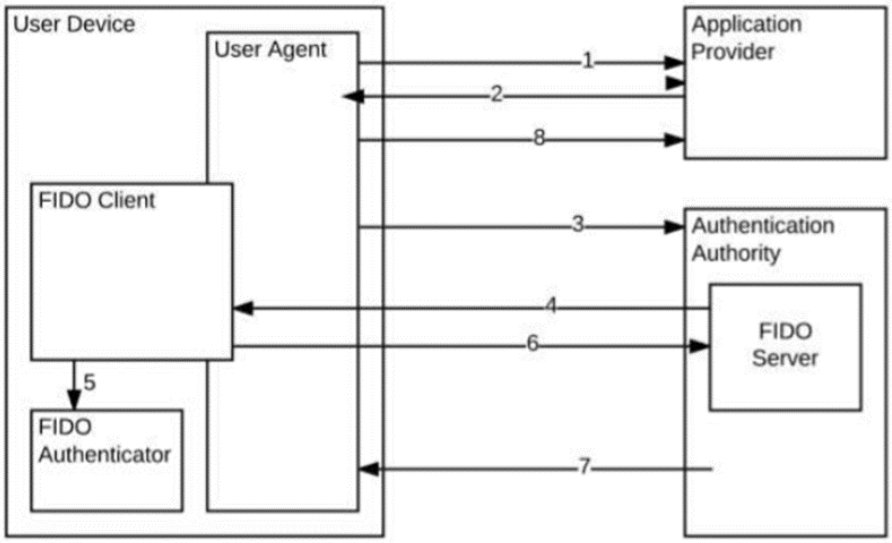
47. Another instance of the accused product is Google Wallet (also known as Google Pay), which includes functionality to biometrically verify a user during authentication of a smartphone. Google Pay is operable on a range of devices, including, at least all recent smartphones that run the Android OS, such the Google Pixel line of smartphones. Current and previous versions of Google Pay, and Google devices such as the Pixel that use Google Pay, alone and together, are further non-limiting instances of the Accused Products.

48. The Accused Products practice the claims of the Patents-in-Suit to improve security and/or the shopping experience of Google's users, and to improve Google's position in the market.

49. Google directly infringes the Patents-in-Suit through the operation of the foregoing as directed and control by Google. The Accused Products practice the claims of the Patents-in-Suit to improve the user experience of Google's customers and those of subscribing developers, and to improve Google's position in the market with respect to identity and access management, operating as an identity provider, and other products, services, and subscriptions.

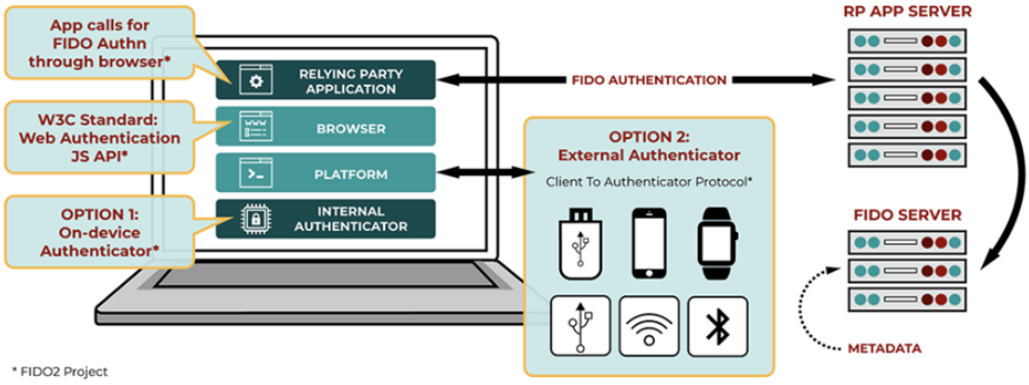
50. Google directly infringes the Patents-in-Suit by creating and utilizing a universal platform password-less architecture incorporating authenticators, including the Android OS and Titan Security Key, the Chrome browser, online Google accounts, and Google Identity, which controls the actions of authenticators and the dissemination of tokens and other such access messages, offering services, applications subscriptions and other such resources hosted by separate systems which are accessed via tokens provided by Google Identity, and offering businesses and developers identity and access management services which entail requesting user authentication and receiving tokens in a manner directed and controlled by Google.

51. Google's password-less architecture verifies a user during authentication of an integrated device – *i.e.*, a phone with Android OS 9 or higher or Titan Security Key - when a user wants to sign into an application or service developed by Google or a business / developer subscribing to Google Identity. **Exhibit 18** and **Exhibit 19**. Google's universal platform password-less architecture is built upon the FIDO and OpenID connect protocols. OpenID Connect and FIDO are two separate standards that can be combined. *See* Enterprise Adoption Best Practices Integrating FIDO & Federation Protocols, December 2017, **Exhibit 20**. When combined, the login procedure resembles that shown below.



Id., page 10

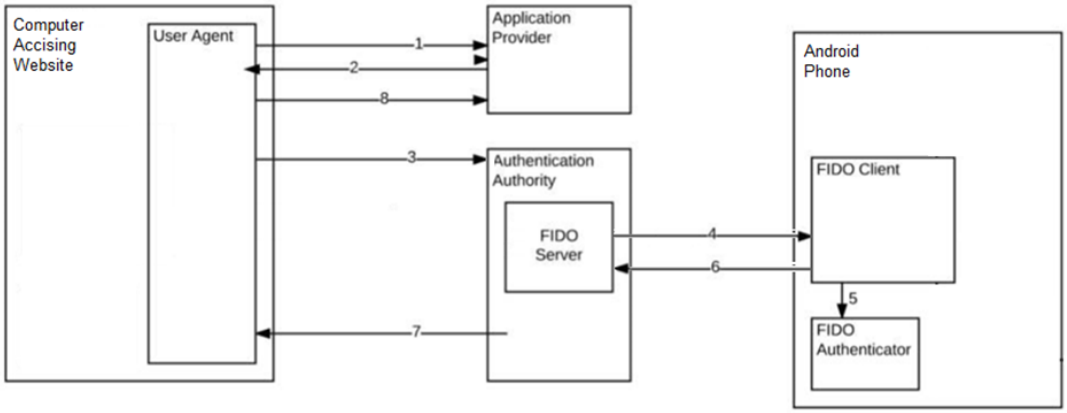
52. The figure above presents a scenario where the user is authenticated using the same device they are using to access a website or other application. This is not always the case, as the below figure shows.



See **Exhibit 21**

53. As shown above, an "External Authenticator" can be used, such as a user's Android phone. Google's "User Your Phone to Sign In" and passkey allows Google account holders to sign into application, websites and services by tapping on their phone. *See* Sign in with Google prompts - Android - Google Account Help., **Exhibit 22** ("When you sign in to your

Google Account, you can tap a notification on your phone to confirm it's you."); and **Exhibit 23** ("Let's say a user has an Android device and created a passkey on a website via Chrome. The passkey is saved and synced among Android devices, but not other ecosystems. When the user tries to sign in to the same website on macOS 13 Safari, there are no passkeys saved on the Mac. The user can still use the Android device to sign in by selecting to use a passkey from a second device. Safari shows a QR code that the user can scan using the Android phone, select the passkey and verify with their screen lock."). Accordingly, a process that may begin on a traditional computer may continue on a user's Android phone. The following diagram modifies the first figure above to reflect the second figure:



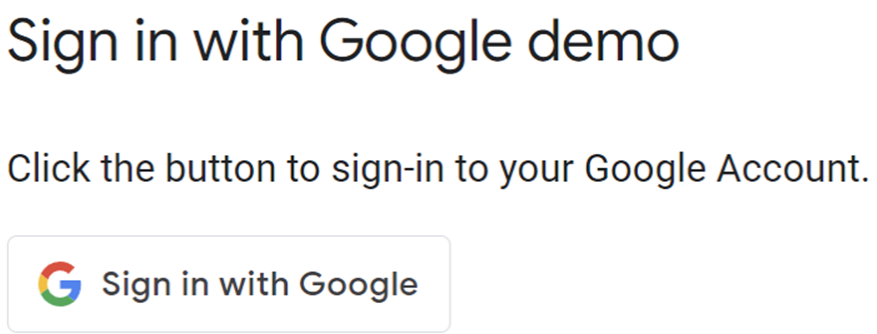
54. The steps shown in the figure above are implemented by Google Identity, the user's Android phone, the user's browser to relay messages from Google Identity to the phone, and the website, application, or service being accessed.

55. Step 1 begins when the user attempts to access a website, application, or service using either "Sign-in with Google" or a passkey. *See* **Exhibit 24** ("Sign in with Google helps [developers] to quickly and easily manage user authentication on [their] website. Users sign into a Google Account, provide their consent, and securely share their profile with [the developer's]

platform."); and **Exhibit 18** ("Passkeys are a safer and easier replacement for passwords. With passkeys, users can sign in to apps and websites with a biometric sensor (such as a fingerprint or facial recognition), PIN, or pattern, freeing them from having to remember and manage passwords.").

56. To receive the benefit of quickly and easily managing user authentication utilizing "Sign-in with Google", the website must display a "Sign in with Google" button, which is generated by the Google Identity Services JavaScript library, or provide the user the option to sign in with a passkey. **Exhibit 25** ("Put it another way, the Sign in with Google button must be generated by the Google Identity Services JavaScript library now. The button rendering API allows you to customize the color, shape, text, and size to meet the branding requirements of your website, whereas still stick to Google's guidelines."); and **Exhibit 23.**

57. A functional demonstration of the "Sign in with Google" button is provided in Google Identity documentation, as shown below.

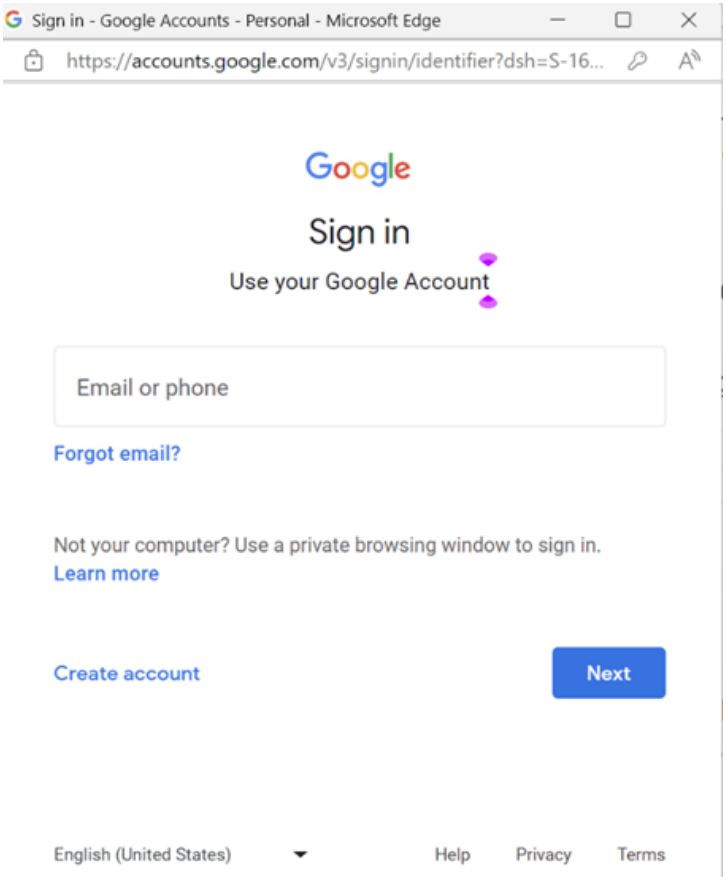


See **Exhibit 24**.

58. Alternatively, a user may be provided the convenience of biometric login without passkeys through of use of Passkeys. **Exhibit 18**. ("Passkeys are a safer and easier replacement for passwords. With passkeys, users can sign in to apps and websites with a biometric sensor

(such as a fingerprint or facial recognition), PIN, or pattern, freeing them from having to remember and manage passwords.") **Exhibit 23.**

59. Step 2 in the figure above involves the presentation of this "Sign in with Google" button to the user. When this button is clicked, the dialog box pictured below is presented to the user.



60. Accordingly, the process has moved from step 2 to step 3, where the website has redirected the browser to Google Identity's FIDO enabled servers and the user has accessed them. The user enters an email and then clicks "next". If the user has activated "Use your phone to sign in" in their Google Account, the following dialog box is presented directing the user to complete the sign on with their phone, thereby moving process along to step 4, where Google Identity servers send a challenge to the FIDO client on the user's Android phone.

61. Google Identity servers then "challenges the user to login with a previously registered device." *See* **Exhibit 26.** The previously registered device may be the user's Android smartphone, such as a Google Pixel device. Since the process is based on the presence of the Android OS, it is the same for any Android phone, including any Pixel model phones or Android phones from other Original Equipment Manufacturers ("OEM"). To register a device as a legitimate, verified device, the user simply signs into a Google account with the Android phone. *See* **Exhibit 22**, ("You'll get Google prompts on any Android phone signed in to your Google Account."). *See also* **Exhibit 27**.

62. Alternatively, if the user opted to sign in passkey, a QR is presented to the user to scan with their Android phone. *See* **Exhibit 23**. Scanning the codes causes the devices to connect. *Id.*

63. Google maintains a list of legitimate devices for each user. The FIDO standard utilized by Google Identity Service incorporates the WebAuthn standard. *See* **Exhibit 28** ("Today, WebAuthn is part of the FIDO Alliance's FIDO2 specifications and the FIDO Alliance runs certificate programs to ensure compliance."). One of the use cases for WebAuthn is decommissioning lost, stolen, and disgarded devices such that "assertions signed by this credential are rejected." *See* Web Authentication: An API for accessing Public Key Credentials - Level 3, Sec. 1.3.5 Decommissioning, **Exhibit 29**. A user may decommission devices they no longer use by signing out of them via their Google Account. *See* **Exhibit 30** (Instructing users how to secure lost, disgareded, or stolen devices by signing out of them.). To prevent account access from a device, and mark it as no longer legitimate, a user must sign out of the device and all session associated with the device. *Id* ("If you want to make sure there's no account access from a device, sign out of all the session with this device name."); and **Exhibit 22** ("To not get

Google Prompts on a device, sign out of your Google Account on that device."). Accordingly, by maintaining a list of devices the user has selected to remain signed in on, Google Identity maintains a list of legitimate integrated devices.

64. Next at step 4, the Chrome browser receives the "authenticatorGetAssertion" from Google Identity and forwards the request to the Titan Security Key or Android phone utilizing the Android OS authenticator. *See* **Exhibit 15** ("Chrome on all desktop platforms supports using passkeys from mobile devices."). Alternatively, if Sign in with Google is being utilized, a analogous is sent directly to the user's Android phone.

65. Android phones include the Android SafetyNet Authenticator, which is FIDO certified. *See* FIDO® Certified - FIDO Alliance, **Exhibit 31**. SafetyNet provides a set of services and APIs to protect against fake users and is present on Google-approved Android devices. *See* **Exhibit 32** ("SafetyNet provides a set of services and APIs that help protect your app against security threats, including device tampering, bad URLs, potentially harmful apps, and fake users."); **Exhibit 33** ("Android devices offer a "SafetyNet API," which is part of the Google Play Services layer installed on Google-approved Android devices. ").

66. The SafetyNet Authenticator is accessed via a FIDO client that uses the FIDO2 API for Android. *See* **Exhibit 19** ("The FIDO2 API allows Android applications to create and use strong, attested public key- based credentials for the purpose of authenticating users. The API provides a WebAuthn Client implementation, which supports the use of BLE, NFC, and USB roaming authenticators (security keys) as well as a platform authenticator, which allows the user to authenticate using their fingerprint or screenlock.") Using these APIs, the SafetyNet Authenticator can be located. In operation, the SafetyNet Authenticator utilizes the native capacities of the Android OS to provide a secure authenticator. *See* **Exhibit 34** (("The typical

way to develop secure authenticator on Android mobile devices (smartphones and tablets) is to use a secured hardware-backed operating environment... This includes technology such as TEE ("Trusted Execution Environment") that performs cryptographic and other sensitive operations including digital signing and biometric data processing used to support FIDO functionality... Android Keystore allows app developers to store cryptographic keys in a container and use them in cryptographic operations via APIs. Android also offers protection of the fingerprint sensor data via a TEE, which allows for encryption and cryptographic authentication... Adding a small application to complement some function that are necessary to perform as UAF 1.1 authenticator enables Android Keystore with hardware-backed key attestations and fingerprint sensor to become a secure FIDO UAF 1.1 authenticator."). The Android OS runs on all Android phones (such as the Pixel), and thus provides such devices with the necessary capabilities for passwordless FIDO Passkey authentication via Google Identity Service.

67. This brings the process to step 5, wherein the user is authenticated. When "Sign in with Google" is being utilized the user is prompted to complete a biometric "challenge," which requires receiving scan data from a biometric scan and comparing the scan data to biometric data persistently stored in a tamperproof format discussed above. A similar challenge is presented in when signing on with passkey. *See* **Exhibit 23.**

68. Devices utilizing the Android OS persistently store biometric data in a tamper proof format. Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE." *See* **Exhibit 35**. When following these guidelines, requiring acquisition and recognition to occur within the TEE means that the biometric data never leaves the

TEE. Android's TEE, called Trusty, "uses ARM's TrustzoneTM to virtualize the main processor and create a secure trusted execution environment" isolated from the rest of the system. *See* **Exhibit 36**. Accordingly, the biometric data, which never leaves the TEE, also never leaves the Trustzone housing, Trusty. Keeping biometric data within the Trustzone, Android phones persistently store biometric data in a tamper proof format.

69. Additionally, Android phones require user consent to enroll a fingerprint. *See* **Exhibit 37**. As enrolling fingerprints on Android phones require entering PIN / Passcode / Password to evidence user consent, Android phones store biometric data of user in a tamper proof format unable to be subsequently altered.

70. Furthermore, access to the biometric hardware on Android devices is controlled by Fingerprint HIDL. *See* **Exhibit 35**. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. *See id.*

71. In order to perform biometric verification of the user, Android OS authenticators utilized within Google's universal platform password-less architecture causes the device to prompt a user for biometric verification and receive scan data from a biometric scan.

72. When the user is biometrically verified using the fingerprint sensor, the process proceeds to step 6 where a FIDO passkey is used to sign the challenge. Signing the is accomplished utilzing a information within memory that can only ba accessed by a correspnding access key provided by an extenral application. The FIDO CTAP specification incorporates the WebAuthn Specification. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 38**. A public key credential refers to a public key credential source, which includes a credential ID. *Id.* The credential ID uniquely identifies its public key credential source. *Id.* In addition to the credential ID, each public key credential source contains a "credential

private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party. *Id.* Authenticators within the Android OS, therefore, will store within memory a credential comprising a private key of an asymmetric key pair and a credential ID uniquely identifying the private/public key pair to which the private key belongs.

73. The credentials stored by the Android OS authenticator can only be accessed with the appropriate access key. During a WebAuthn authentication ceremony, the Android authenticator receives an "authenticatorGetAssertion", issued by Google Identity, containing the RP ID. *Id.* "A public key credential can only be used for authentication with the same entity (as identified by the RP ID) it was registered with." *Id.* When generating a response, therefore, the authenticator will only retrieve credentials corresponding to the RP ID provided to it by Google Identity in the authenticatorGetAssertion request. *Id.* Therefore, the RP ID is an access key.

74. The credential (i.e. Passkey) used to generate the signature within the request is synced with all of a user's Android phones. *See* **Exhibit 15** ("Passkeys are stored when the user creates a passkey on an Android device, and synced; their passkeys are synch'd wth user's other Android devices...") The passkey, accordingly, is not unique to any particular device, but rather backed up and shared across devices.

75. Passkeys in the Google Password Manager are always end-to-end encrypted. *See* **Exhibit 39.** When a passkey is backed up, its private key is uploaded only in its encrypted form using an encryption key that is only accessible on the user's own devices. *Id*. Without access to the private key, such an attacker cannot use the passkey to sign into its corresponding online account. *Id*. Accordingly, Android phones must contain a secrete decryption value (i.e., the encryption key only accessible on the user's own device) to decrypt and use synced and

backed up passkeys. If this decryption value was altered, it would longer be able to decrypt the passkey for use. As such, Android phones contain a secret decryption value in a tamper proof format unable to subsequently altered.

76. The passkey is held securely within the keystore until it unlocked following biometric verification of the user and used to "sign the service's challenge". See **Exhibit 26**; *see also* **Exhibit 40 (**"When generating or importing a key into the Android KeyStore, you can specify that the key is only authorized to be used if the user has been authenticated. The user is authenticated using a subset of their secure lock screen credentials (pattern/PIN/password, biometric credentials)."). Accordingly, by utilizing Fingerprint HIDL in combination with the KeyStore, phone utilzing the Android OS securely sign challenges received from Google Identity only after successful biometric verification.

77. When using a Titan Passkey or the passkey functionality of the Android OS, step 6 concludes with transferring the signed challenge back the user computer over bluetooth. **Exhibit 23**. The FIDO standard requires all communications with BLE authenticators be encrypted. *See* **Exhibit 41**. FIDO compliant BLE capable authenticators, accordingly, include a receiver-decoder circuit ("RDC") enabling encrypted communications.

78. At step 7 the signed challenge is then sent to Google Identity Servers and verified. Authentication is a service provided by the FIDO server incorporated into Google Identity, and the credential ID is necessary for Google's FIDO server to perform the authentication function. Upon receiving the response (i.e., enablement signal), the server will use the credential ID to locate the appropriate public key to verify a signature generated with the private key held by the authenticator. *Id*. As the proper credential ID is needed for Google's FIDO server to authenticate a user, and the credential ID is included within a response to a get request having the appropriate

relying party ID received from the Google's FIDO server, the response to the authenticatorGetAssertion request generated by the authenticator is an enablement signal enabling authentication by Google's FIDO server. The authenticator, accordingly, generates an enablement signal enabling one or more of an application, a function and a service on a device associated with an external RDC Of course, a critical component of verifying the challenge is verifying that it came from a legitimate device, i.e., one in which the user is currently signed on with their Google Account.

79. The responsibility for sending responses received from an authenticator via BLE or NFC falls upon the WebAuthn Client. *See* **Exhibit 15**. Google identifies its Chrome browser as a WebAuthn client by noting it supports the use of passkeys from mobile devices, including permitting the use of an Android phone as a roaming authenticator on Windows. *Id.* As such, Chrome will forward the enablement signal received from a roaming authenticator to Google's FIDO server.

80. Identifying a device as legitimate or not necessitates some form of device ID uniquely identifying the device. Phones utilizing the Android OS also persistently store a device ID code uniquely identifying the phone in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered. The authenticator integrated into the Android OS supports the Device-bound Public Key Webauthn extension (*devicePubKey*). **Exhibit 39.** Device bound public keys are part of a hardware bound key pair that is used to identify devices. Each time a user authenticates with their Android phone, Google Identity servers will receive a public key uniquely identifying the Android phone. With this unique device ID, Google Identity Services can determine if the Android phone is a legitimate device. Rather, the device-bound key pair enables a device ID, in the form of the device-bound public

key stored on the user's device, to returned with the signed challenge to ensure it originated from a legitimate device. As device-bound public keys are not synced, "observing two passkey signatures with the same device-bound public key is a strong signal that the signatures are generated by the same device." *Id.* On the other hand, if a relying party observes a device-bound public key it has not seen before, this may indicate that the passkeys has been synced to a new device. *Id* ("This *device-bound* private key is unique to the passkey in question, and each response includes a copy of the corresponding device-bound public key.").

81. Device Bound Public Keys are stored in a format that when altered causes verification to fail. When a Device Bound Public Key is present, the integrated authenticator within the Android OS causes the phone to store a private key bound to the device. **Exhibit 29** at § 10.2.2.2 (Defining making a credential with a device bound public key as including "5. Let dpk be the newly created or existing device public key, in COSE_Key format in the same fashion as for the user credential's credentialPublicKey when the latter is conveyed in attested credential data. 6. Let devicePrivateKey be the newly created or existing device private key.")) The public key corresponding to the private key is returned to the relying party and saved. **Exhibit 29** at § 10.2.2.3.1 (Stating registration at the relying party includes step "6. Create a new device-bound key record … add this device-bound key record to the devicePubKeys member of the new credential record.").) When processing an authentication request received from Google Identity, the Android OS authenticator creates a signature with the private key associated with the device-bound public key and then sends the signature and the device-bound public key back to Google Identity for verification. *Id*. at § 10.2.2.2 (Defining authentication as including "9. Let dpkSig be the result of signing the assertion signature input with devicePrivateKey. 10. Output dpkSig as the extension's unsigned extension output.").) Upon receipt of the authentication response, the

Google Identity extracts the device bound public key from the response and uses it to verify the signature. *Id.* at § 10.2.2.3.2 (Defining Relying Party verification of the authentication assertion as including "3. Extract the contained fields from attObjForDevicePublicKey: aaguid, dpk, scope, nonce, fmt, attStmt. 4. Verify that signature is a valid signature over the assertion signature input (i.e. authData and hash) by the device public key dpk.")) If the device bound public key were changed at any time, Google Identity would not be able to verify the signature as it would no longer correspond to the authenticator's device bound private key. Accordingly, by being part of a key pair, the device bound public key is in a format unable to be subsequently altered.

82. Of course, if both the private key and public key were altered, then the signature could be verified. In such a situation, however, the altered device bound public key would not match any of the device bound public keys stored by the Relying Party (i.e., Microsoft and Google). *See Id.* at § 10.2.2.3.2 (Steps 5 and 6 detailing, during an authentication ceremony, comparing the received device bound public key to a list of stored device bound public keys, where the lack of a match indicates a new device.). The Relying Party, accordingly, would treat the altered device bound public key as representing a new device and not allow the request absent further user verification. Accordingly, by being recorded by the relying party, device bound public keys are further placed in format unable to be subsequently altered.

~~83.~~ Device-bound public keys are further placed in tamper proof format unable to be subsequently altered by requiring user consent to be created. A device-bound public keys are created when either first using an Android OS authenticate or when authenticating with a new device. **Exhibit 39.** When an authenticator is first used to authenticate an new credential is created, which requires user verification. **Exhibit 41**, at § 6.1 ("For backwards compatibility,

platforms must be aware that FIDO_2_0 (aka CTAP2.0) authenticators always require some form of user verification for authenticatorMakeCredential operations. If a platform attempts to create a non-discoverable credential on a CTAP2.0 authenticator without including the "uv" option key or the pinUvAuthToken parameter that authenticator will return an error. In contrast, a FIDO_2_1 (aka CTAP2.1) authenticator with the makeCredUvNotRqd option ID (set to true) in the authenticatorGetInfo response structure, will allow creation of non-discoverable credentials without requiring some form of user verification.”).) Device-bound public keys are also created when user a authenticates. **Exhibit 39.** “The device-bound key pair is created and stored on-demand. That means relying parties can request the devicePubKey extension when getting a signature from an existing passkey, even if devicePubKey was not requested when the passkey was created.”). Authentication is the process of verifying the user, and thus requires user consent to complete.

~~84.~~ Google Identity also includes a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices. At the end of step 7, if Google Identity Services verify the signed challenge and that the public key corresponds to a legitimate device, an access message is returned in the form of an authorization code.

85. Finally at step 8, the user agent utilizes the authentication code to log the user into the website by exchanging the authorization code for the appropriate token. If resources in addition to the website are to be accessed, the Authorization Code may be exchanged for an ID Token or an Access Token. To make the exchange, Google requires the client agent (i.e., website loaded in the computer’s browser) send a POST request containing the authorization code received from Google, as well as a client ID and client secret obtained when the developer registered the User Agent with Google Identity Services. *See* **Exhibit 42**. The information

contained in the ID Token is then used to querry the developer's database to determine if the user exists, and if so, to start sesssion for the user given access to the website or application. *Id.* ("After obtaining user information from the ID Token, you should querry your app's database. If the user already exsits in your database, you should start an appication session for that user if all login requirements are met by the Google API response."). The Authorization Code received from Google Identity Services is a message permitting access to the application or website by being exchangable for an ID Token used to allow access.

86. If, however, the User Agent needs to access a resource such file in Google Drive or other resource, the authentication code may be exhanged for an Access Token. *Id.* ("One of the advantages of using OAuth 2.0 for authentication is that your application can get permission to use other Google APIs on hehalf of the user (such as YouTube, Google Drive, Calendar, or Contacts) at the same time as you authenticate the user."). To exchange the Authorization Code for an Access Token, Google requires the client agent send a POST request containing the authorization code received from Google, as well as a client ID and client secret obtained when the developer registered the User Agent with Google Identity Services. *Id.* The Authorization Code received from Google Identity Service, thus, is a message permitting access to files and applications associated with Google APIs.

87. As the foregoing shows, Google Identity is at the center of Google's universal platform password-less architecture. It receives messages sent by applications, services, and websites in a manner prescribed by Google. It directs the action of Android OS authenticators, and it issues bear tokens in the manner that Google chooses. Accordingly, Google directs and controls the actions of developers and partners wishing to receive the benefit of utilizing or being part of the Accused Product.

88. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees have also either complied with the marking provisions of 35 U.S.C. § 287, or else were excused from the obligation to mark for the reason that § 287 does not apply.

a) Google Pay / Google Wallet and Android Phones Pre-Loaded Therewith

89. Google directly infringes the Patents-in-Suit by, for example, selling Pixel phones preloaded with Google Pay. Google also actively induces infringement the Patents-in-Suit by disseminating Google Wallet and Google Pay as the default payment app of Android OS. When an Android phone equipped with Google Pay in the lock state is presented to make a contactless payment transaction, the user infringes the Patents-in-Suit.

90. Android phones can make contactless payments. *See* **Exhibit 43** and **Exhibit 44** ("Google Pay can be used to make NFC transactions in stores…"). To do so, users can hold their Android phone close to a payment terminal. If the device is locked, the user will be prompted to unlock the phone, which can be done with a fingerprint (or other biometric authentication mechanism available and supported). *See* **Exhibit 45**.

91. Unlocking a phone with a fingerprint, for example, requires receiving scan data from a biometric scan and comparing the scan data to biometric data persistently stored in a tamperproof format. On Android devices, access to the biometric hardware is controlled by Fingerprint HIDL. "Android uses Fingerprint Hardware Interface Definition Language (HIDL) to connect to a vendor-specific library and fingerprint hardware (for example, a fingerprint sensor)." *See* **Exhibit 35**.

92. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. *Id*. (providing a listing of methods, none of which allowing for the alternation of biometric

data.). Keeping fingerprint and other biometric data within a portion of the Trustzone only accessible by Fingerprint HIDL, which lacks a method for altering biometric data, Android devices persistently store 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.

93. Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE." Android Open-Source Project: Fingerprint HIDL, *Id.* Android's TEE, called Trusty, "uses ARM's TrustzoneTM to virtualize the main processor and create a secure trusted exaction environment" isolated from the rest of the system. *See* **Exhibit 36**. Accordingly, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing, Trusty. Keeping biometric data within the Trustzone, Android phones persistently store biometric data in a tamper proof format.

94. When the user is biometrically verified with the fingerprint sensor and the phone unlocked, an EMV Payment Token stored on the phone is sent via NFC to the payment terminal. "When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value." *See* **Exhibit 46**. A user with multiple device or multiple Google account on the same device can add the same card to each of their accounts and devices. *Id*. Though each user tokenizes a card using the same PAN, each wallet receives a unique number. *Id*.

95. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number. *Id.* As each wallet receives a unique DPAN, i.e., Token, a token is a device ID uniquely identifying an Android device.

96. Provisioning is the process "whereby a Payment Token and related data are delivered to the Token Location." EMV Payment Tokenisation Specification, Technical Framework v2.2, page 11. Android phones support Host Card Emulation (HCE) to enable contactless payment transactions. "When NFC card emulation is provided using a secure element, the card to be emulated is provisioned into the secure element on the device through an Android application." *See* **Exhibit 43.**

97. Since 2018, all Google's Pixel phones have included a "Titan M" chip, a tamper-resistant hardware enclave, also known as a Secure Element ("SE"). See **Exhibit 47**. An SE, according to the U.S. Payments Forum, is "a dynamic environment to store data securely, process data securely and perform communication with external entities securely," that "will not allow unauthorized access." Accordingly, the payment token (DPAN) uniquely identifying an Android phone is stored in a tamperproof format within the Android phone's secure element. After unlocking an Android phone held close to the payment terminal with a fingerprint (or other biometric verification), Google Pay passes the token to the payment terminal instead of the actual card number. *See* **Exhibit 46** ("A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number.")

98. After being received by the payment terminal, the token is forwarded to Token Service Provider. First the token is packaged into a Token Payment Request by the payment terminal and passed to the payment network. *See* **Exhibit 48,** Figure 10.1 and Table 10-1. During transaction routing within the payment network, the Token Payment Request is transformed to a Token Authorization Request, which still contains the token uniquely identifying the Android device. *Id.,* Figure 10.1 and Table 10-3. Accordingly, the payment token sent in the Token Payment Request from the merchant continues to persist during the

token authorization request process. "The Token Authorisation request process continues until De-Tokenisation has been completed." *Id.*, page 86. De-Tokenisation is performed by the token service provider.

99. "Token Service Providers are responsible for a number of discrete functions which may include, but are not limited to: Maintenance and operation of a Token Vault . . . [and] De-Tokenisation". *Id.* A Token Vault is repository that maintains a mapping of the token to the underlying credit card number. *Id.,* page 12 (Defining Token Vault as "A repository that maintains the established Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date and includes Payment Token related data."). By maintaining the token vault, token service providers keep a list of device ID codes uniquely identifying legitimate integrated devices. Accordingly, token service providers are one example of a third-party trusted authority possessing a list of device ID codes uniquely identifying legitimate Android phones.

100. Detokenisation is "the process of converting a Payment Token and Token Expiry Date to its underlying PAN and PAN Expiry Date based on the Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date stored in the Token Vault." By converting the payment token to its underlying account number based on the Payment Token / Token Expiry Date mapping to the underlying PAN / PAN Expiry Date stored in the token vault, the token service provider necessarily authenticates the payment token received from the Samsung Pay preloaded smartphone.

101. After the token has been de-tokenized, the actual credit card number received from the token vault is placed within a PAN Authorization Request which is sent to the bank that issued the credit card. *Id.* Upon receipt of the request, the issuer completes final authorization and sends an authorization response. Accordingly, the authorization request containing the PAN

in place of the payment token allows the user access to the issuing bank's computer software necessary to process and authorize the payment.

The issuing banks then sends a PAN Authorization Response back to the Token Service Provider. A push notification is then sent from the TSP to the Android Phone. *See* **Exhibit 49**, Figures 6, 7, and 11. As the push notification is received in response to processing of the transaction request by the bank, the push notification received indicates allowed access to the banks software necessary to process the transaction.

b. Google's Indirect Infringement of the Patents-in-Suit

102. Google actively induces infringement of the Patents-in-Suit by taking active steps to encourage direct infringement, despite having actual and constructive knowledge about the Patents-in-Suit, as alleged above, and that the induced acts would amount to infringement of the Patents-in-Suit. Specifically, Google actively engaged in encouraging infringement of the Patents-in-Suits by creating, providing and maintaining a substantial knowledge base online, teaching how to use the features and how to integrate its universal platform password-less architecture into various applications, websites, and processes.

103. The knowledge base includes advertising for the infringing features of its password-less architecture.

104. In addition to educating consumers on how to actively engage in infringing uses, Google is actively creating a knowledge base among developers on how to integrate their resources to exploit Google's universal platform password-less architecture. By teaching developers how to integrate their resources into its password-less architecture, Google is assisting in performing the infringing uses of Microsoft Identity.

105. Through integration and developer guides, instructions on Google's websites, and advertising, Google has created and is actively providing and maintaining a knowledge base encouraging infringement of the Patents-in-Suit.

106. Google also actively contributes to infringement of the Patents-in-Suit by providing a native authenticator within the Android OS to allow users to incorporate their devices into Google's universal platform password-less architecture, as these have no substantial non-infringing use, and are especially made for such infringement.

107. As noted *supra* with regards to direct infringement, Titan Security Keys and native authenticator within the Android OS are components of the Accused Products. Accordingly, they are especially made for infringement of the Patents-in-Suit.

CLAIM 1
(Infringement of the 730 Patent)

108. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

109. Proxense has not licensed or otherwise authorized Google to make, use, offer for sale, sell, or import any products that embody the inventions of the 730 Patent.

110. Google infringes at least claims 1, 2, 3, 5, 15, 16, and 17 of the 730 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

111. For example, Google directly infringes at least claims 1, 2, 3, and 5 of the 730 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Google's universal platform password-less architecture incorporating the Android OS integrated authenticator. Under the coordination of Google Identity, the integrated Android OS authenticator performs/executes and provides, a method for verifying a

user during authentication of the device. Google also infringes at least claims 15, 16, and 17 of the 730 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Google's universal platform password-less architecture incorporating Google Identity. The coordination and control provided by Google Identity of the other components within the architecture provides a system for verifying a user during authentication of a device.

112. Google has induced infringement, and continues to induce infringement, of at least claims 1, 2, 3, and 5 of the 730 Patent in violation of 35 U.S.C. § 271 by providing use of its universal platform password-less architecture incorporating integrated Android OS authenticator, Chrome browser, and Google Identity for use by users to access resources offered by Google, including applications, services, and subscriptions. Google also induces infringement of claims 15, 16, and 17 by making Google Identity available for integration with developer applications, and substantial knowledge base teaching developers and business subscribing to Google's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

113. Google contributes to direct infringement of at least claims 1, 2, 3, and 5 of the 730 Patent in violation of 35 U.S.C. § 271(c) by providing use of its universal platform password-less architecture incorporating integrated Android OS authenticator, Chrome browser, and Google Identity for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Google also induces infringement of claims 15, 16, and 17 by making Google Identity available for integration with developer applications, providing the Microsoft Authentication Library, and substantial knowledge base teaching developers and business

subscribing to Google's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

114. Google received actual notice of the 730 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 730 Patent.

115. Since at least the date of service of this Complaint, through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 730 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers and/or end users of the Accused Products to directly infringe the 730 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Google promoting the use of the Accused Product are the public documents discussed supra, which serve no function other than to direct users of the Accused Products toward infringing the 730 Patent.

116. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the 730 Patent, thereby specifically intending for and inducing its customers to infringe the 730 Patent through the customers' normal and customary use of the Accused Products.

117. In addition, Google has indirectly infringed and continues to indirectly infringe the 730 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 730 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

118. The infringing aspects of the Accused Products can be used only in a manner that infringes the 730 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

119. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

120. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Google.

CLAIM 2
(Infringement of 954 Patent)

121. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

122. Proxense has not licensed or otherwise authorized Google to make, use, offer for sale, sell, or import any products that embody the inventions of the 954 Patent.

123. Google infringes at least claims 1, 2, 3, 5, 6, 7, 22, 23, 24, 25, 26, and 27 of the 954 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

124. For example, Google directly infringes at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating integrated Android OS authenticator. Under the coordination of Google Identity, the authenticator performs/executes and provides a method for verifying a user during authentication of the device. Google also infringes at least claims 22, 23, 24, 25, 26, and 27 of the 954 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States access to Google's universal platform password-less architecture incorporating Google Identity. The coordination and control provided by Google Identity Platform of the other components within the architecture provides a system for verifying a user during authentication of a device.

125. Google has induced infringement, and continues to induce infringement, of at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent in violation of 35 U.S.C. § 271 by providing use of its universal platform password-less architecture incorporating integrated Android OS authenticator, Chrome browser, and Google Identity for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Google also induces infringement of claims 22, 23, 24, 25, 26, and 27 by making Google Identity available for integration with developer applications and substantial knowledge base teaching developers and business subscribing to Google's Identity and Access Management services about the features, use and integration of their

resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

126. Google contributes to direct infringement of at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent in violation of 35 U.S.C. § 271(c) by providing use of its universal platform password-less architecture incorporating integrated Android OS authenticator, Chrome browser, and Google Identity for use by users to access resources offered by Google, including applications, services, and subscriptions. Google also induces infringement of claims 22, 23, 24, 25, 26, and 27 by making Google Identity available for integration with developer applications and substantial knowledge base teaching developers and business subscribing to Google's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

127. Google received actual notice of the 954 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 954 Patent.

128. Since at least the date of service of this Complaint, through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 954 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers and/or end users of the Accused Products to directly infringe the 954 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on

how to implement and configure the Accused Products. Some examples of Google promoting the use of the Accused Product are the public documents discussed supra, which serve no function other than to direct users of the Accused Products toward infringing the 954 Patent.

129. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the 954 Patent, thereby specifically intending for and inducing its customers to infringe the 954 Patent through the customers' normal and customary use of the Accused Products.

130. In addition, Google has indirectly infringed and continues to indirectly infringe the 954 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 954 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

131. The infringing aspects of the Accused Products can be used only in a manner that infringes the 954 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

132. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 954 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

133. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 954 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. §

283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Google.

CLAIM 3
(Infringement of 905 Patent)

134. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

135. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or import any products that embody the inventions of the 905 Patent.

136. Google infringes at least claims 1, 2, and 15 of the 905 Patent in violation of 35 U.S.C. § 271 with respect to the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

137. For example, Google directly infringes at least claims 1 and 2 of the 905 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft universal password-less architecture incorporating the integrated Android OS authenticator. Under the coordination of Google identity, the authenticators perform/execute and provide a method for verifying a user during authentication of the device. Google also infringes at least claim 15 of the 905 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering access to sell within the United States Google's universal platform password-less architecture incorporating Google Identity. The coordination and control provide by Google Identity of the other components within the architecture provides a system for verifying a user during authentication of the device.

138. Google has induced infringement, and continues to induce infringement, of at least claims 1 and 2 of the 905 Patent in violation of 35 U.S.C. § 271 by providing use of its universal

platform password-less architecture incorporating the integrated Android OS authenticator, Chrome browser, and Google Idenity for use by users to access resources offered by Google, including applications, services, and subscriptions. Google also induces infringement of claim 15 by making Google Identity available for integration with developer applications and substantial knowledge base teaching developers and business subscribing to Google's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

139. Google contributes to direct infringement of at least claims 1 and 2 of the 905 Patent in violation of 35 U.S.C. § 271(c) by providing use of its universal platform password-less architecture incorporating the integrated Android OS authenticator, Chrome browser, and Google Identity for use by users to access resources offered by Google, including applications, services, and subscriptions. Google also induces infringement of claim 15 by making Google Identity available for integration with developer applications and substantial knowledge base teaching developers and business subscribing to Google's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

140. Google received actual notice of the 905 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 905 Patent.

141. Since at least the date of service of this Complaint, through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 954 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers and/or end users of the Accused Products to directly infringe the 905 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Google promoting the use of the Accused Product are the public documents discussed supra, which serve no function other than to direct users of the Accused Products toward infringing the 905 Patent.

142. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the 905 Patent, thereby specifically intending for and inducing its customers to infringe the 905 Patent through the customers' normal and customary use of the Accused Products.

143. In addition, Google has indirectly infringed and continues to indirectly infringe the 905 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 954 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

144. The infringing aspects of the Accused Products can be used only in a manner that infringes the 905 Patent and thus have no substantial non-infringing uses. The infringing aspects

of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

145. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

146. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 905 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 905 Patent by Google.

CLAIM 3
(Infringement of 402 Patent)

147. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

148. Proxense has not licensed or otherwise authorized Google to make, use, offer for sale, sell, or import any products that embody the inventions of the 402 Patent.

149. Microsoft infringes at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271 with respect to the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

150. For example, Google directly infringes at least claim 1 of the 042 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Google's universal platform password-less architecture incorporating the integrated Android OS authenticator, Titan Security Key authenticator, and Google Identity. Under the coordination of Google Identity, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

151. Google has induced infringement, and continues to induce infringement, of at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271 by making Google Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

152. Google contributes to direct infringement of at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271(c) by Google Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

153. Google received actual notice of the 042 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 042 Patent.

154. Since at least the date of service of this Complaint, through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 042 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers and/or end users of the Accused Products to directly infringe the 042 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the Accused Products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Google promoting the

use of the Accused Product are the public documents discussed supra, which serve no function other than to direct users of the Accused Products toward infringing the 042 Patent.

155. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the 042 Patent, thereby specifically intending for and inducing its customers to infringe the 042 Patent through the customers' normal and customary use of the Accused Products.

156. In addition, Google has indirectly infringed and continues to indirectly infringe the 905 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the Accused Products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 042 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

157. The infringing aspects of the Accused Products can be used only in a manner that infringes the 042 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

158. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 042 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

159. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 042 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. §

283, Proxense is entitled to a permanent injunction against further infringement of the 042 Patent by Google.

CLAIM 5
(Infringement of 289 Patent)

160. Proxense repeats and realleges all preceding paragraphs, as if fully set herein.

161. Proxense has not licensed or otherwise authorized Google to make, use, offer for sale, sell, or import any products that embody the inventions of the 289 Patent.

162. Google infringes at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

163. For example, Google directly infringes at least claims 14 and 16 of the 289 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Google's universal platform password-less architecture incorporating the integrated Android OS authenticator, Titan Security Key authenticator, and Google Identity. Under the coordination of Google Identity, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

164. Google has induced infringement, and continues to induce infringement, of at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271 by making Google Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

165. Google contributes to direct infringement of at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271(c) by making Google Identity available for integration with

developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

166. Google received actual notice of the 289 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 289 Patent.

167. Through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 289 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 289 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the accused products. Some examples of Google promoting the use of the accused products are packaging Google Identity with Android phones and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 289 Patent.

168. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 289 Patent, thereby specifically intending for and inducing its customers to infringe the 289 Patent through the customers' normal and customary use of the Accused Products.

169. In addition, Google has indirectly infringed and continues to indirectly infringe the 289 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 289 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

170. For example, Google is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 289 Patent, including claims 14 and 16. Google continues to sell and offer to sell these products in the United States after receiving notice of the 289 Patent and how its products infringe that patent.

171. The infringing aspects of the Accused Products can be used only in a manner that infringes the 289 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

172. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 289 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

173. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 289 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 289 Patent by Google.

CLAIM 6
(Infringement of the 960 Patent)

174. Proxense repeats and realleges all preceding paragraphs, as if fully set herein.

175. Proxense has not licensed or otherwise authorized Google to make, use, offer for sale, sell, or import any products that embody the inventions of the 960 Patent.

176. Google infringes at least claims 14 and 16 of the 960 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

177. For example, Google directly infringes at least claims 14 and 16 selling access to, and/or offering to sell access to within the United States Google's universal platform password-less architecture incorporating the integrated Android OS authenticator, Titan Security Key authenticator, and Google Identity. Under the coordination of Google Identity, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

178. Google received actual notice of the 960 Patent at least as early as the filing of this Complaint. Google performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness that the acts would constitute direct and/or indirect infringement of the 960 Patent.

179. Through its actions and continued actions, Google has indirectly infringed and continues to indirectly infringe the 960 Patent in violation of 35 U.S.C. § 271(b). Google has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 960 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product

descriptions, operating manuals, and other instructions on how to implement and configure the accused products. Some examples of Google promoting the use of the accused products are packaging Google Identity with Android phones and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 960 Patent.

180. Google does so knowingly and intending that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 960 Patent, thereby specifically intending for and inducing its customers to infringe the 960 Patent through the customers' normal and customary use of the Accused Products.

181. In addition, Google has indirectly infringed and continues to indirectly infringe the 960 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 960 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

182. For example, Google is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 960 Patent, including claims 14 and 16. Google continues to sell and offer to sell these products in the United States after receiving notice of the 960 Patent and how its products infringe that patent.

183. The infringing aspects of the Accused Products can be used only in a manner that infringes the 960 Patent and thus have no substantial non-infringing uses. The infringing aspects

of those instrumentalities otherwise have no meaningful use, let alone any meaningful noninfringing use.

184. Proxense has been injured and seeks damages to adequately compensate it for Google's infringement of the 960 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

185. Upon information and belief, Google will continue to infringe (both directly and indirectly) the 960 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 960 Patent by Google.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants infringe one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendants' infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendants' infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: May 2, 2023

Respectfully submitted,

/s/ David L. Hecht
David L. Hecht (**Co-Lead Counsel**)
dhecht@hechtpartners.com
Maxim Price (*pro hac vice* forthcoming)
mprice@hechtpartners.com
Conor B. McDonough (*pro hac vice* forthcoming)
cmcdonough@hechtpartners.com
Yi Wen Wu (*pro hac vice* forthcoming)
wwu@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
Bryce T. Barcelo
bbarcelo@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

EXHIBIT 17

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC, *Plaintiffs*, v. MICROSOFT CORPORATION, *Defendants*.	Civil Action No. 6:23-cv-00319 **JURY TRIAL REQUESTED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Proxense, LLC ("Proxense" or "Plaintiff") hereby sets forth its Complaint for patent infringement against Defendant Microsoft Corporation ("Microsoft" or "Defendant"), and states as follows:

NATURE OF THE CASE

1. This action is for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, et seq. As further stated herein, Proxense alleges that Microsoft infringes one or more claims of patents owned by Proxense. Accordingly, Proxense seeks monetary damages and injunctive relief in this action.

THE PARTIES

2. Plaintiff Proxense, LLC is a Delaware company with its principal place of business at 689 NW Stonepine Drive, Bend, Oregon 97703.

3. On information and belief, Microsoft is a corporation organized and existing under the laws of the State of Washington, with a principal place of business in this district located at 10900 Stonelake Boulevard, Suite 225, Austin, Texas 78759.

JURISDICTION AND VENUE

4. This Court has exclusive subject matter jurisdiction over this case pursuant to 28 U.S.C. §§ 1331 and 1338(a) on the grounds that this action arises under the Patent Laws of the United States, 35 U.S.C. § 1 et seq., including, without limitation, 35 U.S.C. §§ 271, 281, 284, and 285.

5. This Court has personal jurisdiction over Microsoft because it has conducted and continues to regularly conduct business within the State of Texas and this District. Microsoft has purposefully and voluntarily availed itself of the privileges of conducting business in the United States, the State of Texas, and this District by continuously and systematically placing goods into the stream of commerce through an established distribution channel with the expectation that they will be purchased by consumers in this District. Microsoft directly and/or through intermediaries (including distributors, sales agents, and others), ships, distributes, sells, offers to sell, imports, advertises, makes, and/or uses its products (including but not limited to the products accused of infringement herein) in the United States, the State of Texas, and this District.

6. Upon information and belief, Microsoft conducts business within the State of Texas and in this district, and has designated Corporation Service Company d/b/a CSC − Lawyers Incorporating Service Company, 211 E. 7th Street, STE 620, Austin, Texas 78701-3218, as its agent for service of process in this district.

7. On information and belief, Microsoft has been registered to do business within the State of Texas under Texas Secretary of State File Number 0010404606 since about March 1987.

8. On information and belief, Microsoft employs one or more of its data centers in this district in furtherance of infringing acts in this district since at least 2008. For example, Microsoft maintains data centers in this district, located at: 5150 Rogers Road, San Antonio,

Texas 78251, 5200 Rogers Road, San Antonio, Texas 78251,[1] and 3823 Wiseman Boulevard, San Antonio, Texas 78251.[2]

9. On information and belief, Microsoft has operated data centers supporting Microsoft products and services within the State of Texas, and within this district, since at least 2008. Microsoft is building at least three additional data centers in this district, including two data centers located at: 3545 Wiseman Boulevard, San Antonio, Texas 78251, and another data center located at 15000 Block Lambda Drive, San Antonio, Texas 78245. Upon information and belief, Microsoft's data centers, including those in this district, include computer hardware (*e.g.*, memory and processors) that store and execute software that performs some of the actions that infringe on the patents in the lawsuit. On information and belief, Microsoft has employed, is employing, and is offering to employ individuals in this district in furtherance of infringing acts in this district. On information and belief, these employees have direct personal knowledge about the accused products and Microsoft's infringing activities. For example, Justin Santos, Senior Cloud Security Architect, purporting according to his LinkedIn profile to be working at Microsoft in Austin, Texas, describes that he "[d]rive[s] the use and consumption of Microsoft's … Identity products and services in highly regulated industries – Financial, Healthcare, Federal, and State and Local Government across the US as a part of Microsoft's new Security Solution Area within Customer Success United (CSU)." These data centers which Microsoft operates constitute a regular and established physical presence in the district, including, but not limited to, ownership of or control over property, inventory, or infrastructure.

---

[1] *See* https://www.datacenterhawk.com/providers/microsoft-azure (last accessed April 28, 2023).
[2] *See* https://www.virtualbx.com/industry-news/san-antonio-microsoft-reaches-mid-point-on-86m-expansion-in-westover-hills/ (last accessed April 28, 2023).

10. On information and belief, Microsoft has operated permanent office facilities within the State of Texas, and within this district, since at least 2000. The offices Microsoft maintains in this district include locations at 10900 Stonelake Boulevard, Suite 225, Austin, Texas 78759[3] and Concord Park II, 401 East Sonterra Boulevard, Suite 300, San Antonio, Texas 78258.

11. Microsoft operates offices in Austin, Texas for the purpose of selling, promoting, maintaining, and providing support for a suite of products, including the accused products.

12. On information and belief, Microsoft maintains a "Corporate Sales Offices" in Austin, Texas at the following address: 10900 Stonelake Boulevard, Suite 225 Austin, TX, 78759; and Microsoft maintains a "Corporate Sales Office" in San Antonio, Texas at the following address: Concord Park II 401 East Sonterra Boulevard, Suite 300, San Antonio, TX, 78258.

13. On information and belief, one or more of the Accused Products are used, offered for sale, and sold in this district, including by Microsoft and by "Microsoft-certified resellers" (e.g., Heart of Texas Network Consultants, located at 703 Willow Grove Rd., Waco, Texas 76712).

14. On information and belief, Microsoft operated at least ten physical stores throughout Texas, some of which were in this district, from 2009 until they were all closed in 2020. During that time period, Microsoft had physical stores that sold Microsoft's products at least at the following addresses: (a) 3309 Esperanza Crossing, Austin, TX 78758 and (b) 15900 La Cantera Parkway The Shops at La Cantera San Antonio, TX 78256.

---

[3] *See* https://news.microsoft.com/2000/01/05/microsoft-opens-austin-texas-facility/ (last accessed April 28, 2023).

15. Proxense's causes of action arise directly from Microsoft's business contacts and other activities in the State of Texas and this District.

16. Microsoft has derived substantial revenues from its infringing acts within the State of Texas and this District.

17. In other recent actions, Microsoft has either admitted or not contested that this federal judicial district is a proper venue for patent infringement actions against it. *See*, *e.g.*, *Thompson v. Microsoft Corp.*, No. 1:19-cv-00680-RP, Dkt. No. 6; *Panther Innovations v. Microsoft Corp.*, No. 6-20-cv-01071, Dkt. No. 14; *Exafer Ltd. v. Microsoft Corp.*, No 1-20-cv-00131, Dkt. No. 15; *WSOU Investments, LLC v. Microsoft Corp.*, No. 20-cv-00464, Dkt. No. 20; *Zeroclick, LLC v. Microsoft Corp.*, No. 20-cv-00272, Dkt. No. 14; and *California Institute of Technology v. Microsoft Corp.*, No. 21-cv-00276, Dkt. No. 22.

18. Venue is proper in the Western District of Texas pursuant to 28 U.S.C. §§ 1391 and 1400(b) because Microsoft maintains regular and established places of business in this district and has committed acts of infringement within this district giving rise to this action.

19. Microsoft has committed acts of infringement in this District and does business in this District, including making sales and/or providing service and support for customers and/or end-users in this District. Microsoft purposefully and voluntarily sold one or more infringing products with the expectation they would be purchased in this District. These infringing products have been and continue to be purchased in this District. Thus, Microsoft has committed acts of infringement within the United States, the State of Texas, and this District.

20. Furthermore, Microsoft maintains corporate sales offices in this district, which, on information and belief, provide sales and support for the infringing products.

PATENTS-IN-SUIT

21. On January 8, 2013, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,352,730 (the "730 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 730 Patent is attached hereto as **Exhibit 1**.

22. On November 11, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,886,954 (the "954 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 954 Patent is attached hereto as **Exhibit 2**.

23. On March 26, 2016, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,298,905 (the "905 Patent") entitled "Biometric Personal Data Key (PDK) Authentication." A true and correct copy of the 905 Patent is attached hereto as **Exhibit 3**.

24. On February 4, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,646,042 (the "042 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 042 Patent is attached hereto as **Exhibit 4**.

25. On June 13, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,679,289 (the "289 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 289 Patent is attached hereto as **Exhibit 5**.

26. On September 11, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 10,073,960 (the "960 Patent") entitled "Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use." A true and correct copy of the 960 Patent is attached hereto as **Exhibit 6**.

27. Proxense is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the 730, 954, 905, 042, 289, and 960 Patents (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Proxense also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

28. The technologies of the Patents-in-Suit were invented by John Giobbi and, for some of the patents, David Brown. The 730, 954, 905, and 989 Patents generally cover systems, devices, and methods for an integrated device that persistently stores biometric data for a user in a tamper-resistant format. Subsequently, scan data collected from a user (*e.g.*, a fingerprint) can be compared against the stored biometric data. Once the user has been biometrically verified by the integrated device, a code can be wirelessly transmitted for authentication. The 042, 289, and 960 Patents generally cover systems, devices, and methods of utilizing personal digital keys for verifying a user in order to enable applications, functions, or services.

FACTUAL ALLEGATIONS

I. TECHNOLOGY BACKGROUND

29. Authentication is the process by which the identity of a user is confirmed on a device, including computers, tablets, and phones. When a person is authenticated, the goal is to verify that the credentials presented are authentic. For years, users were authenticated with usernames and passwords. However, with the amount of sensitive personal and financial information currently stored on personal devices and the growing number of devices and services that people use on a regular basis and that require regular authentication, and the rise of biometric readers and high-speed networks, there was a need to implement improved

authentication architectures. The Username and password method is not an ideal authentication mechanisms because people tend to pick low security passwords that are easy to remember, they tend to reuse the same password across multiple devices and services, they tend not the change the password, and they sometimes write the password down on paper or type out the password in public where their device screen can be seen by those around them. This method is also time consuming and inconvenient from a user experience perspective, especially when a user needs to try several passwords or needs to type out a high security (long and complex) password on the small keyboard of a portable device. For all of these reasons and many more, a better architecture is one that relies less on the users' memory.

30. One such architecture is "federated authentication" (also known as "federated identity"), which relies on an external trusted system to authenticate users. In a federated authentication solution, the system being accessed must request authentication of the user from the external system that is used to authenticate users. The external system authenticating the user will then communicate successful authentication back to the system being accessed. Successful authentication is communicated between the two systems with the issuance security tokens containing claims about user authentication. Upon successful authentication of a user, the external system issues a security token which can be exchanged for access to the other system. One such federated architecture is OpenID Connect. This method relies less on user memory because they need to use their username and password significantly less often.

31. While OpenID connect limited the use of passwords, it did not eliminate them. Authentication protocols geared towards eliminating passwords include WebAuthn and its derivative, FIDO2, an open authentication standard developed by the FIDO alliance. WebAuthn, and the derivative protocol FIDO2, utilize an asymmetric key pair to authenticate a device.

Possession and control of the device verifies the identity of the user. The device, referred to as an authenticator, generates a private/public key pair and a credential ID uniquely identifying the key pair. The public key and credential ID are sent to the authentication server – called in the protocol the "relying party". The private key is held by the authenticator. During authentication, the authenticator sends a signature generated with its private key and the credential ID identifying the private key used to generate the signature. The relying party (i.e., authentication server) uses the credential ID to retrieve the matching public key. The signature is then verified with the public key. Upon successful verification of the signature, the relying party issues an authentication response.

32. WebAuthn and federated protocols can be combined. When combined, the system to be accessed by the user requests authentication by a WebAuthn / FIDO 2 server. The server issues an authentication request to the user's authenticator. The authenticator responds by providing a signature and credential ID to the WebAuthn/FIDO2 server. If the signature is verified, the WebAuthn/FIDO2 server informs the OpenID connect of successful authentication. The OpenID connect server then sends a security token to be used to access the system requesting authentication.

33. Attempting to eliminate the use of passwords, Microsoft has developed a universal platform "password-less" architecture. The architecture is universal in that it works across platforms, such as iOS, Android, Windows, and Xbox. It is password-less in that passwords have been replaced with the use of authenticators approved or provided by Microsoft. Incorporating OpenID Connect, Microsoft's architecture relies on the issuance of security tokens. The hub of Microsoft's universal platform password-less architecture is Microsoft Identity Platform, which is the evolution of Azure Active Directory. The Microsoft Identity

Platform receives authentication requests from external systems, coordinates the action of authenticators, and issues security tokens.

II. PROXENSE AND ITS INNOVATIVE TECHNOLOGIES

34. Proxense was founded in 2001.[4] From approximately 2004-2012, Proxense developed, *inter alia*, mobile payment technologies and commercial products, employing over thirty engineers, and investing many millions of dollars in product development and other research and development efforts. Foundational capabilities of Proxense's technologies included a secure element, biometrics captured and stored thereon, retrieval of biometrics and token passing to a trusted third party, and completion of a mobile payment transaction.

35. Proxense also developed sophisticated, proprietary, proximity-based detection, authentication, and automation technology, built on the concept of wirelessly detecting, authenticating, and communicating with personal digital keys ("PDKs"). Proxense's technology enabled PDKs to run for as long as two years on tiny batteries. "ProxPay" technology also included biometrically-based user and device authentication options, the ability to conduct biometric-verified transactions without sending or exposing the underlying biometric data or storing it anywhere except the PDK, and the incorporation of a registration for maintaining or verifying the PDK. Significant financial and engineering resources were deployed to make this possible. The resulting developments became primary differentiators of Proxense's product line, and significant elements on which its business was built.

36. John Giobbi is the founder and CEO of Proxense. He is an experienced product designer and prolific inventor (a named inventor on approximately 200 patents, including the

[4] The company was formally incorporated as an LLC in 2001 under the name Margent Development LLC; in 2005, the business was renamed to Proxense LLC.

asserted patents), with over 35 years of experience as an entrepreneur and product development executive. For example, Mr. Giobbi was a Senior Vice President at WMS Gaming, and managed over 200 staff; in his six-year tenure at that company, its market capitalization soared from approximately $80 million to about $1 billion. Mr. Giobbi was also the founder and President of Prelude Technology Corp. and InPen.

37. The innovative, visionary nature of Proxense's technology was recognized in the media, beginning in mid-2008, when, The Bulletin featured a story on Proxense's mobile payment technology, titled "A pint-sized virtual wallet." Andrew Moore, The Bulletin (May 7, 2008), **Exhibit 7**. The story describes a future that greatly resembles the present-day, including a "wireless wallet" and "fingerprint" verification, including the use of such technology to pay for goods using such wireless methods protected by biometric measures like a fingerprint. In 2009, Trend Hunter ran a similar story titled "Virtual Biometric Wallets," featuring Proxense and Mr. Giobbi. Michael Plishka, Trend Hunter (January 4, 2009), **Exhibit 8**.

38. Another 2009 article, ran in DARKReading, a publication in InformationWeek's IT Network, also featured the company and Mr. Giobbi in an article titled "Startup May Just Digitize Your Wallet." George V. Hulme, DARKReading (February 8, 2009), **Exhibit 9**. The DARKReading article described that Proxense was "in the process of bringing to market a proximity-based communications device that aims to provide a way to securely share information and conduct payments." Proxense's Personal Digital Keys (PDKs) were described as "carried by users, perhaps even within a cell phone, and can security hold data and manage authentication." Mr. Giobbi explained that "the data within the PDK also can be protected by additional layers of authentication, such as biometric…"

39. It would be years until products like Azure Active Directory and Microsoft Identity launched, and accordingly Proxense's technology was years ahead of the industry.

40. Today, Proxense holds at least 80 patents on related technology, including digital content distribution, digital rights management, personal authentication, biometric data management and mobile payments. Proxense continues to prosecute new patents on its proprietary technology.

III. INFRINGEMENT ALLEGATIONS

1. Proxense's Interactions with Microsoft

41. In 2010, Proxense engaged in discussions with Microsoft for the purpose of potentially integrating Proxense's proprietary secure authentication technology utilizing biometric authentication into Microsoft products.

42. On July 29, 2016, counsel for Proxense sent a letter to Microsoft, advising it as to Proxense's "over 30 patents" included as an attachment, including the Patents-in-Suit, and further advising of "another 20+ US patent applications pending." A copy of the letter and list of patents attached thereto is attached as **Exhibit 10**.

43. Since at least that time, *i.e.* on or about July 29, 2016, Microsoft has had actual notice of the Patents-in-Suit and the scope of their claims as of at least their dates of issue.

44. Microsoft has also had knowledge of the infringing nature of its activities, or at least a willful blindness regarding the infringing nature of its activities, since at least Proxense's making Microsoft aware of the Patents-in-Suit as early as 2016, but at least as of the public filing of this Complaint. This follows where Proxense included with its July 29, 2016 correspondence a written comparison between Proxense's claimed inventions and Microsoft's products, including details of Microsoft's infringing activity. Microsoft was also aware of Proxense's proprietary

technology at least as early as 2010, when Proxense disclosed details of these technologies during discussions with Microsoft at that time.

45. Despite Microsoft's knowledge of the Patents-in-Suit, detailed knowledge of Proxense's proprietary technology, and Microsoft's knowledge that it infringed the Patents-in-Suit, or, at the very least a willful blindness to the fact that Microsoft infringes Proxense's patents, Microsoft continued to infringe the claims of the Patents-in-Suit. Microsoft's infringement has been and continues to be willful since at least 2016. Microsoft released the Azure Active Directory platform and its evolution into the Microsoft Identity platform with the intent they would be used to infringe the Patents-in-Suit.

2. The Accused Products

46. Through its own actions, and the actions of its customers and user, which Microsoft directs and controls, Microsoft has manufactured, used, marketed, sold, offered for sale, and exported from and imported into the United States a universal platform password-less architecture that directly and/or indirectly infringes (literally or via the doctrine of equivalents) the Patents-in-Suit.

47. Three primary components make up the infringing architecture. The first is the Microsoft Identity Platform (also known as Azure Active Directory), which coordinates the actions of the other components by authenticating users and issuing various bearer tokens. The second is an authenticator permitting user verification by Microsoft Identity Platform. During verification, Microsoft Identity Platform issues commands to the authenticator (called "requests"). Operation of the authenticator, accordingly, is controlled by Microsoft Identity Platform. The third component of the system is a resource, such as an application, website, or subscription, requesting authentication of the user. During user login, the resource sends requests to a URL provided by

Microsoft and in a form dictated by Microsoft. The resource then listens for a reply at a callback URL the resource registered with Microsoft. As with the requests, the callbacks are in the form dictated by Microsoft. The resources are hosted by devices and/or servers separate from Microsoft Identity Platform. Accordingly, the resource and Microsoft Identity Platform are separate and distinct entities and the resource, which is not Microsoft Identity Platform, is the system being accessed.

48. Microsoft utilizes the Microsoft Identity Platform to sign users into Windows 10/11, Xbox consoles, Xbox Game Pass, Office 365, Microsoft Family, and other services and products offered by Microsoft. Microsoft sells access to Microsoft Identity Platform to developers, websites, and corporate clients through various subscriptions. Thus, for a fee, Microsoft Identity Platform becomes an identity provider for applications, businesses, and websites. Selling such identity and access management (IAM) services and controlling the actions of subscribers and users, Microsoft directly and/or indirectly infringes (and literally or under the doctrine of equivalents) the Patents-in-Suit. Furthermore, by utilizing Microsoft Identity Platform for its own product and services, Microsoft directly and/or indirectly infringes (and literally or via the doctrine of equivalents) the Patents-in-Suit.

49. As noted above, Microsoft's infringing universal platform password-less architecture includes an authenticator. One authenticator distributed by Microsoft is Windows Hello, a native component of Windows 10 and 11. Microsoft has distributed variants of Windows Hello that have included functionality to verify a user during authentication of a Windows-compatible device. Since at least November 20, 2018, if not earlier, Windows Hello has enabled password-less sign-in to services and subscriptions offered by Microsoft. *See* **Exhibit 11**. Another authenticator distributed by Microsoft is the Microsoft Authenticator App. Microsoft has

distributed variants of the Microsoft Authenticator App that have included functionality to verify a user during authentication of an Android or iOS compatible mobile device. The current and previous versions of Windows Hello and Microsoft Authenticator, along with devices with them, alone and together, are non-limiting instances of authenticators integrated into the Accused Products.

50. In addition to authenticators developed by Microsoft, authenticators developed by Microsoft's partners may also be incorporated into the Accused Products. To receive the benefit of having their authenticator work on Windows, Microsoft Edge browser, and online Microsoft Accounts, the authenticator must meet the requirements set by Microsoft, including review by Microsoft's engineering team. *See* **Exhibit 12**. By submitting the request for approval, an authenticator developer also enters into a contract with Microsoft in the form of its "Terms of Use," which give Microsoft control over both the terms (which can be changed by Microsoft at any time with no prior notice) and gives Microsoft control over the means by which any such authenticator operates. By setting such requirements, Microsoft directs and controls the actions of its partners.

51. The Microsoft Identity Platform, which directs and controls the actions of the authenticator, is also an element of Accused Product. Microsoft operates and maintains the Microsoft Identity platform, an evolution of the Azure Active Directory platform. When combined with authenticators, such as Windows Hello, Microsoft Authenticator App, and others developed and sold by Microsoft's partners, consumers of Microsoft's products and services receive the benefit of password-less biometric authentication across platforms. For instance, a user may log into and utilize Microsoft Office or their Xbox subscription on their Android phone. Third party developers can purchase identity and access management services from Microsoft to integrate their

applications with Microsoft Identity in order to offer cross platform password-less authentication via biometrics and the use of ID and access tokens to their customers and subscribers. Developers subscribing to Microsoft Identity Platform must register their application or website with Microsoft, request authentication by sending a request to a URL provided by Microsoft and in a format dictated by Microsoft, and listen for a callback provided by Microsoft that contains a message generated by Microsoft in a format controlled by Microsoft. To facilitate such controlled interactions across platforms, Microsoft has developed Microsoft Authentication Library (MSAL). *See* **Exhibit 13**.

52. The Accused Products also include a resource accessed following successful authentication of the authenticator by Microsoft Identity Platform. As noted above, the resource may be an application, website, and/or a subscription offered by Microsoft, a subscribing business, or a subscribing developer. When a user has been authenticated via an authenticator offered by Microsoft or one of its partners, various bearer tokens are returned by Microsoft Identity Platform to the callback URL registered with Microsoft Identity Platform. The bearer token allows access to the application, and as such is an access message. Regardless of whether the resource is an application, a subscription, or a service offered by Microsoft or a subscribing developer or business, the resource is on a system separate and distinct from Microsoft Identity Platform. Distribution of bearer tokens and other such access messages by Microsoft Identity Platform is thus necessary for Microsoft Identity Platform to inform the resource that the user has been successfully authenticated via an authenticator distributed by Microsoft or one of its partners. As the bearer tokens are generated and distributed by Microsoft Identity Platform, Microsoft controls their form and how they are distributed.

53. Through the operation of the foregoing as directed and controlled by Microsoft, the Accused Products practice the claims of the Patents-in-Suit to improve the user experience of Microsoft's customers and those of subscribing developers, and to improve Microsoft's position in the market with respect to Identity and Access Management, operating as an identity provider, along with providing access to other products, services, and subscriptions.

3. Microsoft's Direct Infringement of the Patents-in-Suit

54. Microsoft directly infringes the Patents-in-Suit by creating and utilizing a universal platform password-less architecture incorporating authenticators, including Windows Hello on Windows 10 and 11, Microsoft Authenticator App on Android and iOS devices, and controlling the action of its partners to create authenticators that work on Windows, the Microsoft Edge browser, and online Microsoft accounts, incorporating the Microsoft Identity platform which controls the actions of authenticators and the dissemination of bear tokens and other such access messages, offering services, applications subscriptions and other such resources hosted by separate systems which are accessed via tokens provided by Microsoft Identity Platform, and offering businesses and developers identity and access management services which entail requesting user authentication and receiving tokens in a manner directed and controlled by Microsoft, including the use of Microsoft Authentication Library.

55. Microsoft's password-less architecture verifies a user during authentication of an integrated device. This device may be a computer running Windows 10/11, which includes Windows Hello as a native component. It may also be an Android or iOS device with the Microsoft Authenticator App. Alternatively, it may be an authenticator developed by a partner in accordance with requirements set by Microsoft. Each uses biometrics, such as facial recognition or fingerprints, to verify the user. *See, e.g.*, **Exhibit 14**

56. Following user verification via biometrics, the Microsoft Identity platform utilizes FIDO2 and analogous protocols to authenticate the device and OpenID Connect to permit access to various resources, including Microsoft applications, subscriptions, and services, such as Outlook, Office, Skype, Xbox Live, etc. and those developed by businesses and developers subscribing to Microsoft's Identity and Access Management services. *See* **Exhibit 11.**

57. Windows devices, such as the Microsoft Surface and biometrically enabled laptops produced by Microsoft's partners, persistently store biometric user data. Whether manufactured by Microsoft or its partners, such as Dell, Windows 10 and 11 devices must meet minimum hardware requirements set by Microsoft. *See* **Exhibit 15**. The minimum hardware requirements ensure Windows Hello can utilize specialized hardware and software, such as Virtualization Based Security (VBS) and Trusted Platform Module 2.0 to isolate, protect, and secure the channel by which a user's biometric data is communicated. *See* **Exhibit 16.**

58. For example, when a user elects to use facial recognition for authentication, a face template is generated and encrypted using keys only accessible to the VBS, and then stored on disk. *See id.* Accordingly, facial templates are persistently stored on a Windows device's storage. Likewise, these devices persistently store fingerprint data, but do so instead in the sensor's dedicated memory. *See id.* In all cases, the biometric data is stored so as to prevent unauthorized alterations. This meets the first patented claim limitation of the 730 patent literally or, at least, by the doctrine of equivalents.

59. Android devices with the Microsoft Authenticator App also persistently store biometric data in a tamper proof format. Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) [that] must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint

acquisition, enrollment, and recognition must occur inside the TEE." *See* **Exhibit 17.** When following these guidelines, requiring acquisition and recognition to occur within the TEE means that the biometric data never leaves the TEE. Android's TEE, called Trusty, "uses ARM's TrustzoneTM to virtualize the main processor and create a secure trusted execution environment" isolated from the rest of the system. *See* **Exhibit 29**. Accordingly, the biometric data, which never leaves the TEE, also never leaves the Trustzone housing Trusty. Keeping biometric data within the Trustzone, Android phones persistently store biometric data in a tamper proof format. Furthermore, access to the biometric hardware on Android devices is controlled by Fingerprint HIDL. *Id.*. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. *See id.*

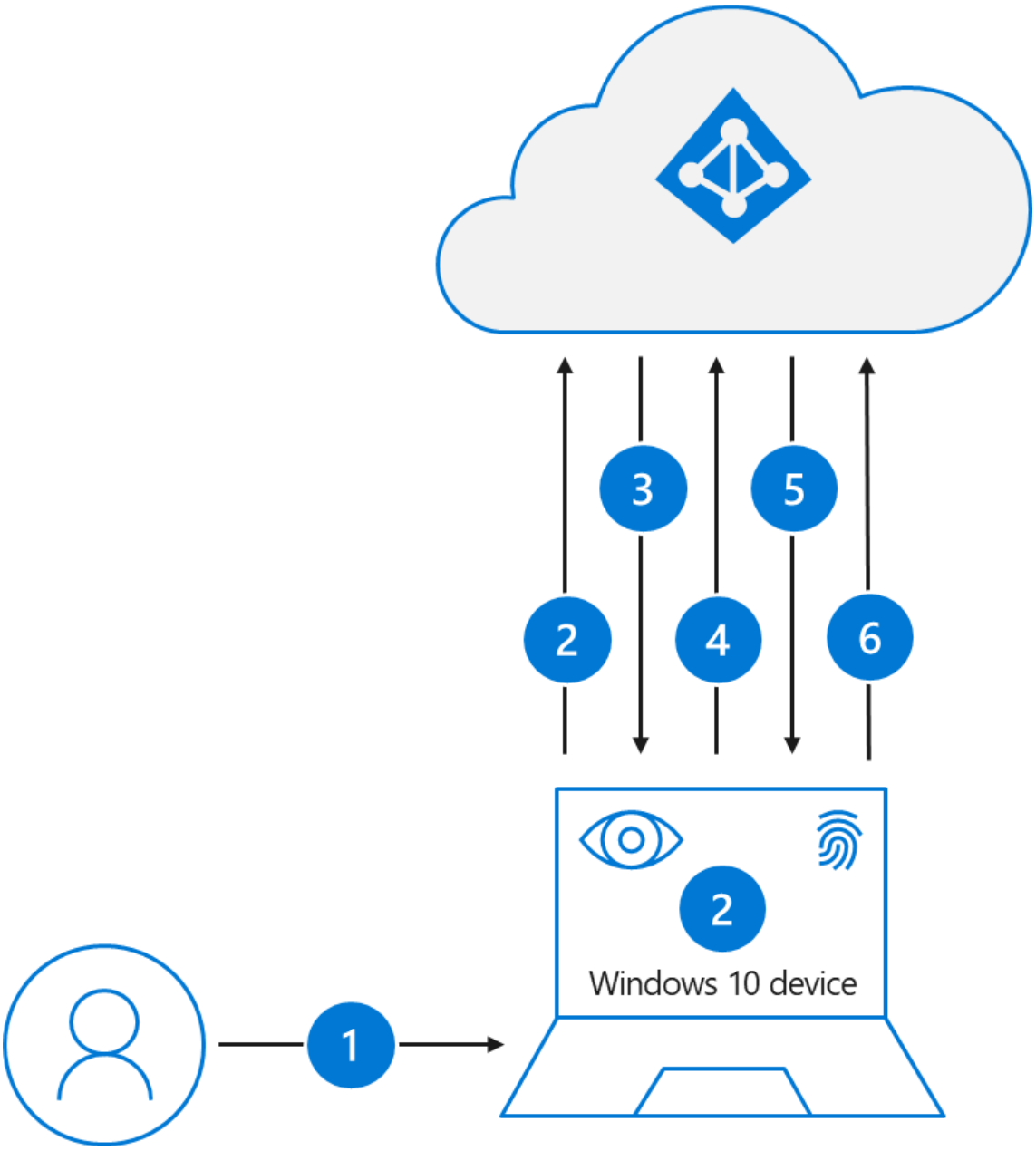
60. iOS devices with the Microsoft Authenticator App also persistently store biometric data in a tamper proof format. Apple's "Secure Enclave is a dedicated secure subsystem … isolated from the main processor to provide an extra layer of security designed to keep sensitive data secure even when the Application Processor kernel becomes compromised." *See* **Exhibit 18**. "During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data." *Id.*. The Secure Enclave thus provides a tamper proof format for sensitive data, such as biometric data, even when a hack or other malicious software compromises the Application Processor.

61. Authenticators developed by Microsoft's partners also store biometric data in a tamper proof format. To receive the benefit of having their authenticator work on Windows, Microsoft Edge browser, and online Microsoft Accounts, a partner's authenticator must meet the requirements set by Microsoft, including being FIDO2 certified. *See* **Exhibit 19**. FIDO compliant authenticators store biometric data of user in tamper proof format unable to be subsequently

altered. Microsoft, accordingly, directs partner authenticators to store biometric data in a tamper proof format. Authenticators developed by Microsoft and its partners persistently store a device ID code uniquely identifying each integrated device. Microsoft's universal platform password-less architecture is based on FIDO2. *See* **Exhibit 16**. Instead of passwords, FIDO2 uses public/private key encryption. *See* **Exhibit 11**. The private key is generated and stored on the authenticator, while the public key is sent to the Microsoft Identity platform. *See id.* When a user attempts to authenticate, Microsoft Identity platform sends a nonce to the authenticator, which is signed with the private key. *See id.* The signed nonce is then returned to the Microsoft Identity Platform and the signature verified with the corresponding public key. For this to work, Microsoft Identity Platform must select the correct public key for the particular authenticator being used. This is accomplished by sending a credential ID indicating which public key to use along with the signed nonce. Accordingly, each public key within Microsoft Identity includes a reference to a credential ID uniquely identifying the device from which it was created. *See* **Exhibit 21**. The credential ID is thus a device ID code that is part of a pair. Being one part of a pair places the Device ID in a tamper proof format on the integrated device.

62. In order to perform biometric verification of the user, authenticators utilized within Microsoft's universal platform password-less architecture causes the device to prompt a user for biometric verification and receive scan data from a biometric scan, which varies depending on how and what the user is logging into.

63. When Windows Hello is used as the authenticator, the prompt for biometric verification occurs after the user dismisses the lock screen, as shown below.

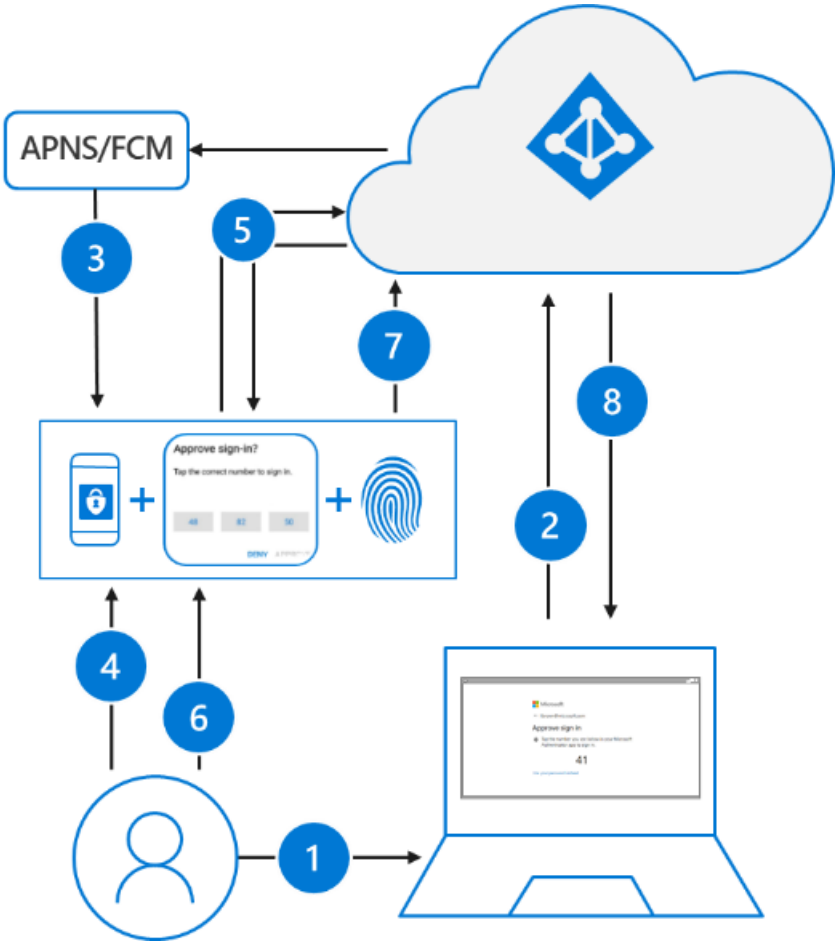


1. A user signs into Windows using biometric or PIN gesture. The gesture unlocks the Windows Hello for Business private key and is sent to the Cloud Authentication security support provider, referred to as the *Cloud AP provider*.
2. The Cloud AP provider requests a nonce (a random arbitrary number that can be used just once) from Azure AD.
3. Azure AD returns a nonce that's valid for 5 minutes.
4. The Cloud AP provider signs the nonce using the user's private key and returns the signed nonce to the Azure AD.

5. Azure AD validates the signed nonce using the user's securely registered public key against the nonce signature. After validating the signature, Azure AD then validates the returned signed nonce. When the nonce is validated, Azure AD creates a primary refresh token (PRT) with session key that is encrypted to the device's transport key and returns it to the Cloud AP provider.
6. The Cloud AP provider receives the encrypted PRT with session key. Using the device's private transport key, the Cloud AP provider decrypts the session key and protects the session key using the device's Trusted Platform Module (TPM).
7. The Cloud AP provider returns a successful authentication response to Windows. The user is then able to access Windows as well as cloud and on-premises applications without the need to authenticate again (SSO).

See **Exhibit 22**.

64. When Microsoft Authenticator App is used as the authenticator, the biometric verification prompt occurs later in the process, as shown below.



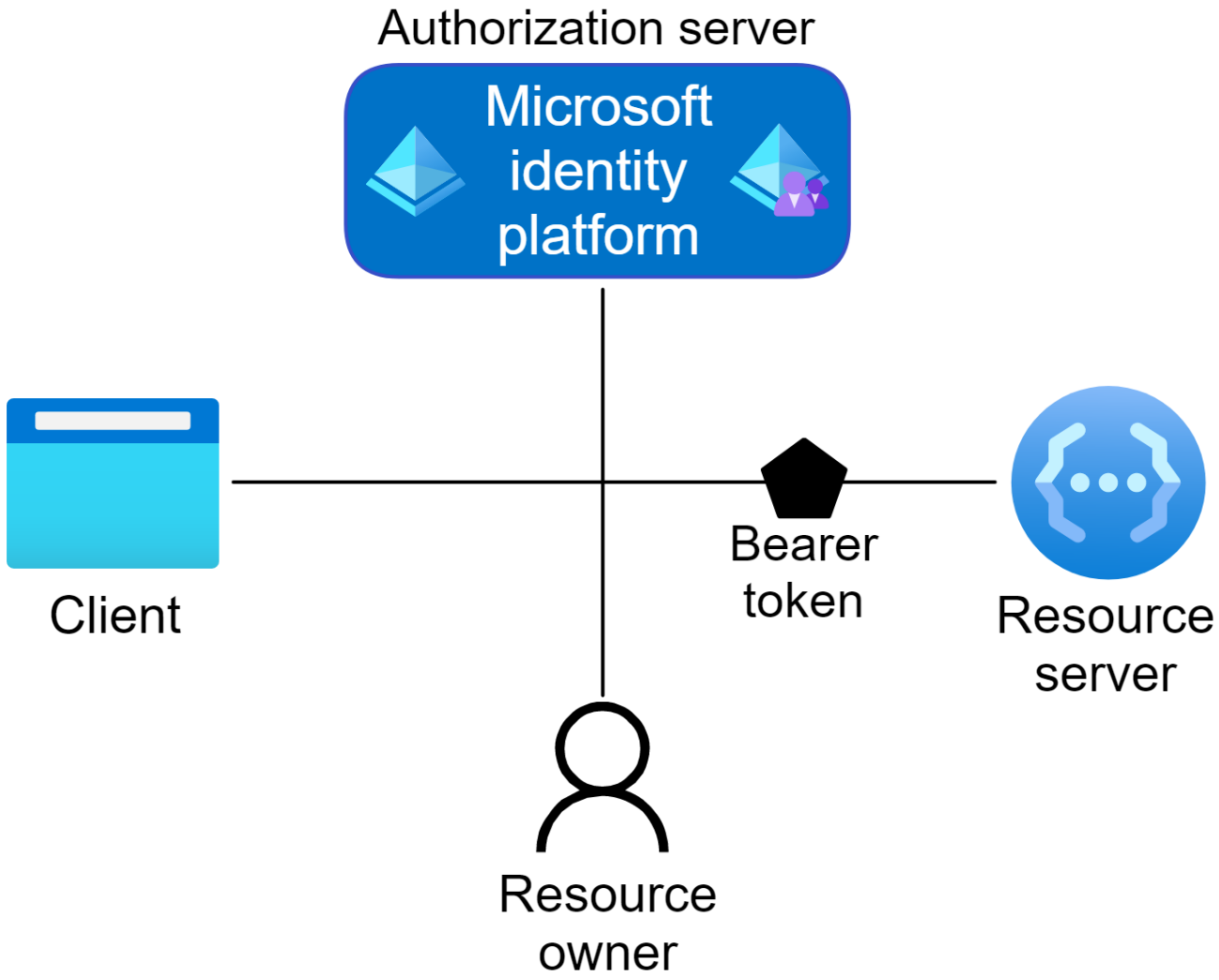
1. The user enters their username.
2. Azure AD detects that the user has a strong credential and starts the Strong Credential flow.
3. A notification is sent to the app via Apple Push Notification Service (APNS) on iOS devices, or via Firebase Cloud Messaging (FCM) on Android devices.
4. The user receives the push notification and opens the app.
5. The app calls Azure AD and receives a proof-of-presence challenge and nonce.

See id. Specifically, at Step 3 "a notification is sent to the app via Apple Push Notification Service (APNS) on iOS devices, or via Firebase Cloud Messaging (FCM) on Android devices." At Step 4, "the user receives the push notification and opens the app." Microsoft prevents the use of the Microsoft Authenticator App on devices without an active security lock, which may be released with biometrics. *See* **Exhibit 23**. Consequently, before opening the App to complete Step 4, the user unlocks the device with biometrics. If the user leaves their device unlocked, App Lock will prompt for a biometric gesture. *See* **Exhibit 24.** Accordingly, regardless of whether the device is locked or unlocked, responding to the notification requires that the device receives data from a biometric scan.

65. The use of Windows Hello, the Microsoft Authenticator App, and partner authenticators within the Microsoft's universal platform password-less architecture is not limited to logging onto a Windows 10/11 computer. For instance, resources, such as applications, services, subscriptions, and websites utilizing the Microsoft Identity Platform for Identity and Access Management natively receive the benefit of utilizing authenticators for password-less user authentication. *See* **Exhibit 25**. As such, the Microsoft Identity Platform permits the use of Microsoft approved authenticators to log into any platform or browser, or confirm any login, with the use of biometric authentication. *See* **Exhibit 18**. Furthermore, developers may utilize Windows Hello on Windows 10/11 computers to protect their Universal Windows Platform (UWP) applications and backend services. *See* **Exhibit 26**. Accordingly, the

request for biometric authentication and the corresponding receipt of biometric scan data occurs when the user logs into any application, device, or service utilizing Microsoft Identity platform for Identity and Access Management.

66. Microsoft Identity platform operates as a third party trusted authority possessing a list of device ID codes uniquely identifying legitimate integrated devices (i.e., Microsoft approved authenticators). Microsoft depicts the relationship between the parties involved in authentication and authorization below.



See **Exhibit 27.**

67. Microsoft Identity takes on the role of the authorization server responsible for authenticating the user. *See id.* Instead of using passwords, it utilizes FIDO2 and analogous protocols to authenticate users. *See* **Exhibit 23.**

68. The protocols employed use public/private key encryption. *See* **Exhibit 11**. Each public key is identified by a unique credential ID. As discussed above, the private key is generated and stored on the authenticator and the public key is sent to Microsoft Identity platform. When a user attempts to authenticate, Microsoft Identity platform sends a nonce to the authenticator, which is signed with the authenticator's private key, returned to Microsoft Identity with a credential ID, and verified with the public key held by Microsoft Identity Platform corresponding to the sent credential ID. *See id.* Sending the credential ID with the signed nonce enables Microsoft Identity Platform to select the correct public key for the particular authenticator being used. A user account, therefore, contains a list of "PassportDevices," (i.e., authenticators) which each entry in the list including a "DeviceId" (i.e., credential ID) and a "PublicKey." *See* **Exhibit 42**. Accordingly, each public key within Microsoft Identity includes a reference to the specific device from which it was created and should be used. *See* **Exhibit 21**.

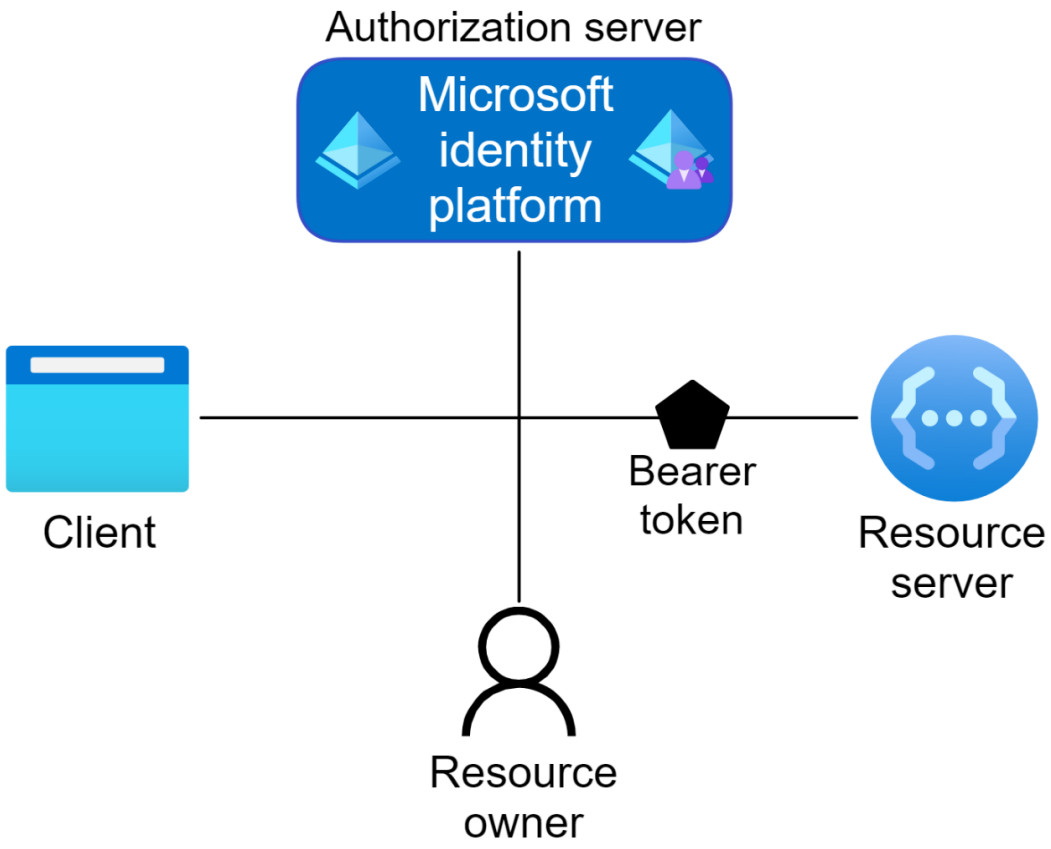
69. Authenticators within Microsoft's universal platform password-less architecture sign the nonce and return it with the credential ID after a determining that the scan data matches the biometric data. As the Microsoft Authenticator App is downloaded to mobile devices, the nonce request (including the device ID codes) is necessarily sent wirelessly. Likewise, computers running Windows 10/11 can wirelessly send the device ID code and nonce request via a wireless connection to a local router or mobile phone.

70. Utilizing OAuth 2.0 and OpenID Connect, Microsoft Identity platform issues access messages in the form of Bearer Tokens to various resources. *See* **Exhibit 36**. Acting as an

authorization server, Microsoft Identity handles the trust relationship between the parties, including issuing security tokens (i.e., Bearer Tokens) for granting access (authorization) after the user has signed in (authenticated). *See* **Exhibit 21**. The Bearer Token is passed between the parties to assure authentication and grant access. There are four types of tokens issued by Microsoft Identity: Access Tokens, ID Tokens, Refresh Tokens, and Primary Refresh Tokens. *See id.* The type of token issued depends on the resource being accessed. Regardless of the resource, the Bearer Tokens received from Microsoft Identity are used to get access to the resource, which may be an application, website, service, subscription, etc. offered by Microsoft or businesses and developers subscribing to Microsoft's Identity and Access Management service and are thus "access messages."

71. The issuance of tokens serving as access messages within Microsoft's universal platform password-less architecture is shown in the figure below. As shown, the resource server providing the application, subscription, service, etc. to be accessed is a separate entity from Microsoft Identity Platform. Thus, regardless of whether the resource is one provided by Microsoft or its customers, the resource server is a separate entity. As such, communication between the resource server and Microsoft Identity Platform is required. This communication is accomplished by the resource server sending a request for authentication using URLs provided by Microsoft and in a form dictated by Microsoft. In many instances, the communication will be mediated via a client, such Microsoft Edge or another web browser, Windows Cloud AP, etc. Regardless of the client, upon receipt of the request form the resource server for user authentication, Microsoft Identity Platform sends requests to a Microsoft approved authenticator to verify the user and sign a nonce. Often the client will facilitate this communication between the Microsoft Identity Platform and the authenticator. After receiving and verifying the signature

generated by the authenticator, Microsoft Identity Platform issues a bearer token. Receipt of the bearer token by the resource server indicates user authentication by Microsoft Identity Platform acting as a third-party with respect to the resource server.



72. As the foregoing shows, Microsoft Identity Platform is at the center of Microsoft's universal platform password-less architecture. It receives messages sent by resource servers in a manner prescribed by Microsoft. It directs the action of Microsoft approved authenticators, and it issues bearer tokens in a manner Microsoft chooses. Accordingly, Microsoft directs and controls the actions of developers and partners wishing to receive the benefit of utilizing or being part of the Accused Product.

73. Proxense has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, any prior assignees and licensees

have also either complied with the marking provisions of 35 U.S.C. § 287, or else were excused from the obligation to mark for the reason that § 287 does not apply.

4. Microsoft's Indirect Infringement of the Patents-in-Suit

74. Microsoft actively induces infringement of the Patents-in-Suit by taking active steps to encourage direct infringement, despite having actual and constructive knowledge about the Patents-in-Suit, as alleged above, and that the induced acts would amount to infringement of the Patents-in-Suit. Specifically, Microsoft actively engaged in encouraging infringement of the Patents-in-Suits by creating, providing and maintaining a substantial knowledge base online, teaching how to use the features and how to integrate its universal platform password-less architecture into various applications, websites, and processes. And Microsoft directly profits from its indirect infringement.

75. The knowledge base includes advertising for the infringing features of its password-less architecture. On its website, Microsoft touts that its customers can "securely sign in with your Microsoft account" with "no username or password required" and that authentication occurs through comparing biometric data such as a fingerprint or facial scan. *See, e.g.*, **Exhibit 11**. In making these statements, Microsoft is advertising the functionality claimed by the Patents-in-Suit. These are just a few of examples of an extensive advertising campaign to make the consumers knowledgeable of the infringing components, functionality, and uses of Microsoft's universal platform password-less architecture.

76. In addition to educating consumers on how to actively engage in infringing uses, Microsoft is actively creating a knowledge base among developers on how to integrate their resources to exploit Microsoft's universal platform password-less architecture. For instance, Microsoft teaches developers how to utilize applications that take advantage of authentication

methods such as the use of biometrics and the use of ID and access tokens. *See, e.g.*, **Exhibit 27**. By teaching developers how to integrate their resources into its password-less architecture, Microsoft is directing third parties to perform the infringing uses of Microsoft Identity.

77. Through integration and developer guides, instructions on Microsoft's websites, and advertising, Microsoft has created and is actively providing and maintaining a knowledge base encouraging infringement of the Patents-in-Suit.

78. Microsoft also actively contributes to infringement of the Patents-in-Suit by providing the authenticators Windows Hello and Microsoft Authenticator App to allow users to incorporate their devices into Microsoft's universal platform password-less architecture, as these have no substantial non-infringing use, and are especially made for such infringement.

79. As noted *supra* with regards to direct infringement, Windows Hello and Microsoft Authenticator App are components of the Accused Products. Accordingly, they are especially made for infringement of the Patents-in-Suit. Furthermore, Windows Hello and Microsoft Authenticator App are software, *i.e.*, a mobile application installed on a smartphone and/or computer. Software, when installed, becomes a component of the device it is installed upon. Accordingly, Windows Hello and Microsoft Authenticator App (when installed on a smartphone and/or device) integrates a user's device into the Accused Product. These software applications are thus especially made for making devices and smartphones into components of the Accused Product, and to practice the methods of the Patents-in-Suit. Moreover, Microsoft includes Windows Hello as a native component of Windows 10/11 installed on Windows compatible devices by Microsoft's OEM partners.

80. At all relevant times, since at least July 2016 (when Microsoft was given notice of all of the limitations of the claims of the Patents-in-Suit that are at issue) to the present, Microsoft

has had full knowledge of the specifications upon which Microsoft relies to develop and maintain its universal platform password-less architecture, the underlying infrastructure (including Microsoft Identity, Microsoft approved authenticators, and resources provided by Microsoft or subscribing developers and business), and all third parties who are in privity with Microsoft. Microsoft did review the relevant specifications and their internal documents in light of, and considering, the claims of the Patents-in-Suit from Proxense's letter; alternatively, Microsoft remained willfully blind to its own infringement by failing to review the relevant specifications and its own internal documents in light of, and considering, the claims of the Patents-in-Suit from Proxense's letter. By publicly releasing instructions, guides, and advertising with knowledge of, or willful blindness to, the fact that those acts will lead to direct infringement by their users and third-party developers, Microsoft has induced and is inducing those parties to participate in Microsoft's infringement.

CLAIM 1
(Infringement of the 730 Patent)

81. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

82. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 730 Patent.

83. Microsoft infringes at least claims 1, 2, 3, 5, 15, 16, and 17 of the 730 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

84. For example, Microsoft directly infringes at least claims 1, 2, 3, and 5 of the 730 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture

incorporating the Microsoft Authenticator App and Windows Hello as authenticators. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device. Microsoft also infringes at least claims 15, 16, and 17 of the 730 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating Microsoft Identity platform. The coordination and control provided by Microsoft Identity Platform of the other components within the architecture provides a system for verifying a user during authentication of a device.

85. As described *supra*, the Microsoft Authenticator App "turns any iOS or Android phone into a strong, passwordless credential." Utilizing the Android operating system, Android Phones having the Microsoft Authenticator App persistently store 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. Starting with Android 10, stored biometric data on Android phones includes a fingerprint and facial recognition. *See* **Exhibit 22**.

86. As to protect biometric data, Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". *See* **Exhibit 17**. Requiring acquisition and recognition to occur inside the TEE, fingerprint data never leaves the TEE. Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted execution environment" isolated from the rest of the system. Accordingly, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing Trusty. Keeping biometric

data within the Trustzone, Android phones persistently store biometric data in a tamper proof format.

87. On Android phones, access to the biometric hardware is controlled by Fingerprint HIDL. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. Keeping fingerprint and other biometric data within a portion of the Trustzone only accessible by Fingerprint HIDL, which lacks a method for altering biometric data, means that Android phones persistently store 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.

88. When the Authenticator App is installed on an iOS device, biometric data would be stored within Apple's Secure Enclave. *See* **Exhibit 30**. Designed to keep sensitive data secure even when compromised, the Secure Enclave provides a tamper proof format for sensitive data.

89. Additionally, both iOS and Android phones require user consent to enroll a fingerprint. *See* **Exhibits 31** and **32.** As enrolling fingerprints on both iPhones and Android phones require entering PIN / Passcode / Password to evidence user consent, iPhones and Android phones store biometric data of user in a tamper proof format unable to be subsequently altered.

90. Windows compatible systems meeting Microsoft's minimum hardware requirements also store data of a user in a tamper proof format unable to be subsequently altered.

91. Microsoft details that the Authenticator App uses key based authentication technology similar to Windows Hello. ("Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology." *See* **Exhibit 43**. Windows Hello is FIDO certified. The FIDO specification incorporates the WebAuthn Specification. *See* **Exhibit 33**. Windows Hello, therefore, uses a key-based authentication technology compliant with the

WebAuthn and FIDO specifications. Utilizing a similar technology, MS Authenticator most use a key-based authentication analogous to the WebAuthn and FIDO protocols.

92. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id*. The credential ID uniquely identifies its public key credential source. *Id*. In addition to the credential ID, each public key credential source contains a "credential private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party (i.e., Microsoft Identity Platform). *Id.* Accordingly, a credential ID uniquely identifies a private/public key pair.

93. The credential ID is used to retrieve the correct public key during authentication ceremonies. *See* **Exhibit 34.** The public key retrieved is used to verify the signature generated with its matching private key held by phone running the Microsoft Authenticator App or Windows 10/11 device natively having Window Hello. *See* **Exhibit 34**. Being part of an asymmetric key pair, the pubic key corresponds to a private key.

94. Altering a Windows Hello or Microsoft Authenticator App credential ID causes authentication to fail. Being FIDO certified, Windows Hello utilizes the WebAuthn protocol. Credential IDs within the WebAuthn protocol are in a tamper proof format unable to be subsequently altered because "all that would happen if an authenticator returns the wrong credential ID, or if an attacker intercepts and manipulates the credential ID, is that the WebAuthn Relying Party would not look up the correct credential public key with which to verify the returned signed authenticator data (a.k.a., assertion), and thus the interaction would end in an error." *See* **Exhibit 34**. As altering the device ID (i.e., Credential ID) causes authentication to fail, the credential ID is necessarily in a tamper proof format unable to be altered. "Passwordless

authentication using the Authenticator app follows the same basic pattern as Windows Hello for Business." *See* **Exhibit 22**. Following the same pattern, altering the device ID stored on the phone by the Authenticator App should produce the same result of causing authentication to fail. As Microsoft controls the protocol utilized by its Identity Platform, including the inability to sync passkeys across devices, users wanting the benefit of biometric authentication via the Microsoft Authenticator App or Windows Hello have no choice but to store on their phone or Windows device a credential ID uniquely identifying the integrated device in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

95. As with the FIDO standards implemented by Windows Hello, the Microsoft Authenticator app utilizes a private key to sign a challenge. *See* **Exhibit 22**. Private keys are notoriously known secret decryption values. If the Authenticator App and Windows Hello have the private keys, the public keys must be held by Microsoft's Identity Platform. By being part of a pair split between the authenticator and Microsoft's Identity Platform, the private key secret decryption value is in a tamper proof format unable to be subsequently altered. As Microsoft controls the protocol utilized by its Identity Platform, including the use of public/private key validation, users wanting the benefit of biometric authentication via the Microsoft Authenticator App or Windows Hello have no choice but to store on their phone or Windows device a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

96. Microsoft describes user authentication via the Authenticator App and Windows Hello as comprising receipt of a proof-of-presence challenge that is completed when the user enters their biometrics. *See* **Exhibit 22**. Entering their biometric necessarily requires receiving scan data from a biometric scan. When the user completes the challenge, the private key held by the phone

or Windows Device is unlocked. Determining if the user successfully completed the challenge necessarily requires comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.

97. As detailed by Microsoft, after the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *See* **Exhibit 22**. The Microsoft Authenticator App operates either on iOS or Android phones. As iOS and Android phones are cellular phones, often possessing Wi-Fi and Bluetooth capability, anything sent to Microsoft Identity Platform will be sent wirelessly – either via Wi-Fi, Bluetooth, or the cellular network. Laptops with Windows have biometric capabilities and are often connected to the internet via Wi-Fi or using a mobile phone as a hotspot. Accordingly, anything sent to Microsoft Identity Platform will be sent wirelessly via the laptop's Wi-Fi connection or connected phones cellular connection.

98. After the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *See* **Exhibit 22**. As previously noted, password-less authentication using the Microsoft Authenticator App follows the same basic pattern as FIDO certified Windows Hello. FIDO incorporates the WebAuthn Protocol. *See* **Exhibit 35**. Accordingly, the challenge sent to the Authenticator App is the equivalent of a FIDO server challenge sent to the Windows Hello authenticator with a WebAuthn authenticatorGetAssertion request. *Id.* The response to the request, therefore, will contain a signature signed by the authenticator's private key and a credential ID (i.e., device ID) identifying which public key to use to verify the signature. *See* **Exhibit 34**. Upon receiving the response, the WebAuthn/FIDO server will use the device ID (i.e., credential ID) to locate the appropriate public key to verify the signature generated with the private key. *See* **Exhibit 34**.

Accordingly, a FIDO/WebAuthn within the Microsoft Identity Platform will authenticate a device ID (i.e., credential ID) sent in response to successful completion of a biometric challenge.

99. As detailed *supra*, upon successful completion of the biometric challenge, a device ID and signature is sent from the authenticator to Microsoft Identity Platform for authentication. The Microsoft Identity Platform utilizes OpenID Connect and Microsoft encourages developers to gain an understanding of the protocol and concepts to add authentication to applications. *See* **Exhibit 36**. Within the protocol, Microsoft identifies its identity platform as an "authorization server" managing "trust relationships" and issuing security tokens applications and APIs use for granting access (i.e. authorization) and authentication. *See* **Exhibit 27**. Accordingly, Microsoft describes its Identity Platform as a third party that operates as a trusted authority for authentication.

100. As noted *supra*, the FIDO server within the Microsoft Identity Platform uses a credential ID operating as a device ID to verify a signature generated with a private key bound to the identified device (i.e., authenticator). Such action is made possible by registering the credentials with an account and associating the account with the credential ID and credential public key. *See* **Exhibit 34**. Accordingly, the Microsoft Identity Platform maintains a listing of legitimate device IDs.

101. Authentication is provided by a FIDO server incorporated into the Microsoft Identity Platform in conjunction with OpenID Connect Authentication Server that is also incorporated into the Microsoft Identity Platform. While OpenID Connect is a federation protocol, it is compatible and complementary with FIDO. "The value of a FIDO authentication capability is amplified by a federated system, where the federation system extends the benefits of a FIDO authentication to applications and services without requiring FIDO to be directly integrated with those applications." *See* **Exhibit 37**. When a federated system, such as OpenID Connect, is

combined with FIDO, the OpenID Provider (OP) sends a FIDO server challenge to an authenticator which is returned as the FIDO Authentication response. *See* **Exhibit 37**.

102. FIDO incorporates the WebAuthn Protocol. Accordingly, the FIDO server challenge sent will a be WebAuthn authenticatorGetAssertion request. The response to the request received will contain a signature generated by the authenticator's private key and a credential ID. *See* **Exhibit 35**. Upon receiving the response, the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify the signature generated with the private key. *See* **Exhibit 34**. Accordingly, a FIDO/WebAuthn server incorporated into Microsoft Identity Platform will authenticate a device ID (i.e., credential ID). After validating the device ID, the FIDO/WebAuthn portion of the Microsoft Identity Platform "redirects the user agent back to the Application Provider with an authentication assertion". *See* **Exhibit 37**.

103. As the Microsoft Identity Platform utilizes OpenID Connect, the authentication assertion will be an ID Token. The ID Token received from Microsoft's Identity platform enables access to an application. The ID Token is thus an access message provided by Microsoft operating as a third party trusted authority allowing access to an application. Should the user also require an access token to access further features of the application, such as files containing stored data, the ID token can be exchanged for an access token. *See* **Exhibit 27**.

104. Further, Microsoft Family enables parents to "designate the age limit for content [a family member] will have permission to access", such as apps and games. *See* **Exhibit 38**.

105. Microsoft has induced infringement, and continues to induce infringement, of at least claims 1, 2, 3, and 5 of the 730 Patent in violation of 35 U.S.C. § 271 by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for

download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claims 15, 16, and 17 by making Microsoft Identity available for integration with developer applications, providing the Microsoft Authentication Library, and substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

106. Microsoft contributes to direct infringement of at least claims 1, 2, 3, and 5 of the 730 Patent in violation of 35 U.S.C. § 271(c) by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claims 15, 16, and 17 by making Microsoft Identity available for integration with developer applications, providing the Microsoft Authentication Library, and a substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

107. Microsoft received actual notice of the 730 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 730 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement,

with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 730 Patent.

108. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 730 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the Accused Products to directly infringe the 730 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Microsoft promoting the use of the Accused Product are packaging Windows Hello with Windows 10/11 and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 730 Patent.

109. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 730 Patent, thereby specifically intending for and inducing its customers to infringe the 730 Patent through the customers' normal and customary use of the Accused Products.

110. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 730 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 730 Patent and despite the fact that

the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

111. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 730 Patent, including claim 1. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 730 Patent and how its products infringe that patent.

112. The infringing aspects of the Accused Products can be used only in a manner that infringes the 730 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

113. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 730 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

114. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 730 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 730 Patent by Microsoft.

CLAIM 2
(Infringement of 954 Patent)

115. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

116. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 954 Patent.

117. Microsoft infringes at least claims 1, 2, 3, 5, 6, 7, 22, 23, 24, 25, 26, and 27 of the 954 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

118. For example, Microsoft directly infringes at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating the Microsoft Authenticator App and Windows Hello as authenticators. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide a method for verifying a user during authentication of the device. Microsoft also infringes at least claims 22, 23, 24, 25, 26, and 27 of the 954 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States access to the Microsoft's universal platform password-less architecture incorporating Microsoft Identity platform. The coordination and control provided by Microsoft Identity Platform of the other components within the architecture provides a system for verifying a user during authentication of a device.

119. As described *supra*, the Microsoft Authenticator App "turns any iOS or Android phone into a strong, passwordless credential." Utilizing the Android operating system, Android Phones having the Microsoft Authenticator App persistently store 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. Starting with Android 10, stored biometric data on Android phones includes a fingerprint and facial recognition. *See* **Exhibit 22**.

120. As to protect biometric data, Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) must never be accessible from

outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". *See* **Exhibit 17**. Requiring acquisition and recognition to occur inside the TEE, fingerprint data never leaves the TEE. Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted execution environment" isolated from the rest of the system. Accordingly, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing Trusty. Keeping biometric data within the Trustzone, Android phones persistently store biometric data in a tamper proof format.

121. On Android phones, access to the biometric hardware is controlled by Fingerprint HIDL. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. Keeping fingerprint and other biometric data within a portion of the Trustzone only accessible by Fingerprint HIDL, which lacks a method for altering biometric data, means that Android phones persistently store 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.

122. When the Authenticator App is installed on an iOS device, biometric data would be stored within Apple's Secure Enclave. *See* **Exhibit 30**. Designed to keep sensitive data secure even when compromised, the Secure Enclave provides a tamper proof format for sensitive data.

123. Additionally, both iOS and Android phones require user consent to enroll a fingerprint. *See* **Exhibits 31** and **32**. As enrolling fingerprints on both iPhones and Android phones require entering PIN / Passcode / Password to evidence user consent, iPhones and Android phones store biometric data of user in a tamper proof format unable to be subsequently altered.

124. Windows compatible systems meeting Microsoft's minimum hardware requirements also store data of a user in a tamper proof format unable to be subsequently altered.

125. Microsoft details that the Authenticator App uses key based authentication technology similar to Windows Hello. ("Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology." *See* **Exhibit 43**. Windows Hello is FIDO certified. The FIDO specification incorporates the WebAuthn Specification. *See* **Exhibit 33**. Windows Hello, therefore, uses a key-based authentication technology compliant with the WebAuthn and FIDO specifications. Utilizing a similar technology, MS Authenticator most use a key-based authentication analogous to the WebAuthn and FIDO protocols.

126. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id.* The credential ID uniquely identifies its public key credential source. *Id.* In addition to the credential ID, each public key credential source contains a "credential private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party (i.e., Microsoft Identity Platform). *Id.* Accordingly, a credential ID uniquely identifies a private/public key pair.

127. The credential ID is used to retrieve the correct public key during authentication ceremonies. *See* **Exhibit 34**. The public retrieved is used to verify the signature generated with its matching private key held by phone running the Microsoft Authenticator App or a Windows 10/11 device natively having Windows Hello. *Id.* Being part of an asymmetric key pair, the public key corresponds to a private key.

128. Altering a Windows Hello or Microsoft Authenticator App credential ID causes authentication to fail. Being FIDO certified, Windows Hello utilizes the WebAuthn protocol.

Credential IDs within the WebAuthn protocol are in a tamper proof format unable to be subsequently altered because "all that would happen if an authenticator returns the wrong credential ID, or if an attacker intercepts and manipulates the credential ID, is that the WebAuthn Relying Party would not look up the correct credential public key with which to verify the returned signed authenticator data (a.k.a., assertion), and thus the interaction would end in an error." *See* ***Id.*** As altering the device ID (i.e., Credential ID) causes authentication to fail, the credential ID is necessarily in a tamper proof format unable to be altered. "Passwordless authentication using the Authenticator app follows the same basic pattern as Windows Hello for Business." *See* **Exhibit 22**. Following the same pattern, altering the device ID stored on the phone by the Authenticator App should produce the same result of causing authentication to fail. As Microsoft controls the protocol utilized by its Identity Platform, including the inability to sync passkeys across devices, users wanting the benefit of biometric authentication via the Microsoft Authenticator App or Windows Hello have no choice but to store on their phone or Windows device a credential ID uniquely identifying the integrated device in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

129. As with the FIDO standards implemented by Windows Hello, the Microsoft Authenticator app utilizes a private key to sign a challenge. *See* **Exhibit 22**. Private keys are notoriously known secret decryption values. If the Authenticator App and Windows Hello have the private key, the public key must be held by Microsoft's Identity Platform. By being part of a pair split between the authenticators and Microsoft's Identity Platform, the private key secret decryption value is in a tamper proof format unable to be subsequently altered. As Microsoft controls the protocol utilized by its Identity Platform, including the use of public/private key validation, users wanting the benefit of biometric authentication via the Microsoft Authenticator

App or Windows Hello have no choice but to store on their phone or Windows device a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

130. Microsoft describes user authentication via the Authenticator App and Windows Hello as comprising receipt of a proof-of-presence challenge completed when the user enters their biometrics. *See* **Exhibit 22**. Entering their biometric necessarily requires receiving scan data from a biometric scan. When the user completes the challenge, the private key held by the phone or Windows device is unlocked. Determining if the user successfully completed the challenge necessarily requires comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.

131. As detailed by Microsoft, after the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *See* **Exhibit 22**. The Microsoft Authenticator App operates either on iOS or Android phones. As iOS and Android phones are cellular phones, often possessing Wi-Fi and Bluetooth capability, anything sent to Microsoft Identity Platform will be sent wirelessly – either via Wi-Fi, Bluetooth, or the cellular network. Laptops are common Windows devices having biometric capabilities and are often connected to the internet via Wi-Fi or using a mobile phone as a hotspot. Accordingly, anything sent to Microsoft Identity Platform will be sent wirelessly via the laptop's Wi-Fi connection or connected phones cellular connection.

132. After the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *See* **Exhibit 22**. As previously noted, password-less authentication using the Microsoft Authenticator App follows the same basic pattern as FIDO certified Windows Hello. FIDO incorporates the

WebAuthn Protocol. *See* **Exhibit 35**. Accordingly, the challenge sent to the Authenticator App is the equivalent of a FIDO server challenge sent to the Windows Hello authenticator with a WebAuthn authenticatorGetAssertion request. The response to the request, therefore, will contain a signature signed by the authenticator's private key and a credential ID (i.e., device ID) identifying which public key to use to verify the signature. *See* **Exhibit 34**. Upon receiving the response, the WebAuthn/FIDO server will use the device ID (i.e., credential ID) to locate the appropriate public key to verify the signature generated with the private key. *Id.* Accordingly, a FIDO/WebAuthn server within the Microsoft Identity Platform will authenticate a device ID (i.e., credential ID) sent in response to successful completion of a biometric challenge.

133. As detailed *supra*, upon successful completion of the biometric challenge, a device ID and signature is sent from the authenticator to Microsoft Identity Platform for authentication. The Microsoft Identity Platform utilizes OpenID Connect and Microsoft encourages developers to gain an understanding of the protocol and concepts to add authentication to applications. *See* **Exhibit 36**. Within the protocol, Microsoft identifies its identity platform as an "authorization server" managing "trust relationships" and issuing security tokens applications and APIs use for granting access (i.e. authorization) and authentication. *See* **Exhibit 27**. Accordingly, Microsoft describes its Identity Platform as a third party that operates as a trusted authority for authentication.

134. As noted supra, the FIDO server within the Microsoft Identity Platform uses a credential ID operating as a device ID to verify a signature generated with a private key bound to the identified device (i.e., authenticator). Such action is made possible by registering the credentials with an account and associating the account with the credential ID and credential public key. *See* **Exhibit 34**. Accordingly, the Microsoft Identity Platform maintains a listing of legitimate device IDs.

135. Authentication is provided by a FIDO server incorporated into the Microsoft Identity Platform in conjunction with an OpenID Connect Authentication Server that is also incorporated into the Microsoft Identity Platform. While OpenID Connect is a federation protocol, it is compatible and complementary with FIDO. "The value of a FIDO authentication capability is amplified by a federated system, where the federation system extends the benefits of a FIDO authentication to applications and services without requiring FIDO to be directly integrated with those applications." *See* **Exhibit 37**. When a federated system, such as OpenID Connect, is combined with FIDO, the OpenID Provider (OP) sends a FIDO server challenge to an authenticator which is returned as the FIDO Authentication response. *Id*.

136. FIDO incorporates the WebAuthn Protocol. Accordingly, the FIDO server challenge sent will be a WebAuthn authenticatorGetAssertion request. The response to the request received will contain a signature generated by the authenticator's private key and a credential ID. *See* **Exhibit 35**. Upon receiving the response, the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify the signature generated with the private key. *See* **Exhibit 34**. Accordingly, a FIDO/WebAuthn server incorporated into Microsoft Identity Platform will authenticate a device ID (i.e., credential ID). After validating the device ID, the FIDO/WebAuthn portion of Microsoft's Identity Platform "redirects the user agent back to the Application Provider with an authentication assertion". *See* **Exhibit 37**.

137. As the Microsoft Identity Platform utilizes OpenID Connect, the authentication assertion will be an ID Token. The ID Token received from Microsoft's Identity platform enables access to an application. The ID Token is thus an access message allowing access to an application that is provided by Microsoft operating as a third party trusted authority. Should the user also

require an access token to access further features of the application, such as files containing stored data, the ID token can be exchanged for an access token. *See* **Exhibit 27**.

138. Further, Microsoft Family enables parents to "designate the age limit for content [a family member] will have permission to access", such as apps and games. *See* **Exhibit 38**.

139. Microsoft has induced infringement, and continues to induce infringement, of at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent in violation of 35 U.S.C. § 271 by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claims 22, 23, 24, 25, 26, and 27 by making Microsoft Identity available for integration with developer applications, providing the Microsoft Authentication Library, and a substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

140. Microsoft contributes to direct infringement of at least claims 1, 2, 3, 5, 6, and 7 of the 954 Patent in violation of 35 U.S.C. § 271(c) by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claims 22, 23, 24, 25, 26, and 27 by making Microsoft Identity available for integration with developer

applications, providing the Microsoft Authentication Library, and a substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

141. Microsoft received actual notice of the 954 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 954 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 954 Patent.

142. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 954 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 954 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Microsoft promoting the use of the accused products are packaging Windows Hello with Windows 10/11 and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 954 Patent.

143. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or

import the accused products, despite its knowledge of the 954 Patent, thereby specifically intending for and inducing its customers to infringe the 954 Patent through the customers' normal and customary use of the Accused Products.

144. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 954 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 954 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

145. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 954 Patent, including claim 1. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 954 Patent and how its products infringe that patent.

146. The infringing aspects of the Accused Products can be used only in a manner that infringes the 954 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

147. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 954 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

148. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 954 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283,

Proxense is entitled to a permanent injunction against further infringement of the 954 Patent by Microsoft.

CLAIM 3
(Infringement of 905 Patent)

149. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

150. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 905 Patent.

151. Microsoft infringes at least claims 1, 2, and 15 of the 905 Patent in violation of 35 U.S.C. § 271 with respect to the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

152. For example, Microsoft directly infringes at least claims 1 and 2 of the 905 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft universal password-less architecture incorporating the Microsoft Authenticator App and Windows Hello as authenticators. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide a method for verifying a user during authentication of the device. Microsoft also infringes at least claim 15 of the 905 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering access to sell within the United States Microsoft's universal platform password-less architecture incorporating Microsoft Identity platform. The coordination and control provide by Microsoft Identity Platform of the other components within the architecture provides a system for verifying a user during authentication of the device.

153. As described *supra*, the Microsoft Authenticator App "turns any iOS or Android phone into a strong, passwordless credential." Utilizing the Android operating system, Android

Phones having the Microsoft Authenticator App persistently store 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. Starting with Android 10, stored biometric data on Android phones includes a fingerprint and facial recognition. *See* **Exhibit 22**.

154. As to protect biometric data, Android's implementation guidelines require tamper-proof "raw fingerprint data or derivatives (for example, templates) must never be accessible from outside the sensor driver or TEE" (trusted execution environment) and "fingerprint acquisition, enrollment, and recognition must occur inside the TEE". *See* **Exhibit 17**. Requiring acquisition and recognition to occur inside the TEE, fingerprint data never leaves the TEE. Android's TEE, called Trusty, "uses ARM's Trustzone™ to virtualize the main processor and create a secure trusted execution environment" isolated from the rest of the system. Accordingly, fingerprint data, which never leaves the TEE, also never leaves the Trustzone housing Trusty. Keeping biometric data within the Trustzone, Android phones persistently store biometric data in a tamper proof format.

155. On Android phones, access to the biometric hardware is controlled by Fingerprint HIDL. The methods enabled by the Fingerprint HIDL do not permit altering biometric data. Keeping fingerprint and other biometric data within a portion of the Trustzone only accessible by Fingerprint HIDL, which lacks a method for altering biometric data, means that Android phones persistently store 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.

156. When the Authenticator App is installed on an iOS device, biometric data would be stored within Apple's Secure Enclave. *See* **Exhibit 30**. Designed to keep sensitive data secure even when compromised, the Secure Enclave provides a tamper proof format for sensitive data.

157. Additionally, both iOS and Android phones require user consent to enroll a fingerprint. *See* **Exhibits 31** and **32**. As enrolling fingerprints on both iPhones and Android phones require entering PIN / Passcode / Password to evidence user consent, iPhones and Android phones store biometric data of user in a tamper proof format unable to be subsequently altered.

158. Windows compatible systems meeting Microsoft's minimum hardware requirements also store data of a user in a tamper proof format unable to be subsequently altered.

159. Microsoft details that the Authenticator App uses key based authentication technology similar to Windows Hello. ("Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology." *See* **Exhibit 43**. Windows Hello is FIDO certified. The FIDO specification incorporates the WebAuthn Specification. *See* **Exhibit 33**. Windows Hello, therefore, uses a key-based authentication technology compliant with the WebAuthn and FIDO specifications. Utilizing a similar technology, the Microsoft Authenticator App most use a key-based authentication analogous to the WebAuthn and FIDO protocols.

160. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id*. The credential ID uniquely identifies its public key credential source. *Id*. In addition to the credential ID, each public key credential source contains a "credential private key". *Id*. "The credential private key is bound to a particular authenticator" and is part of an asymmetric key pair containing a public key returned to a relying party (i.e., Microsoft Identity Platform). *Id*. Accordingly, a credential ID uniquely identifies a private/public key pair.

161. The credential ID is used to retrieve the correct public key during authentication ceremonies. *Id*. The public key retrieved is used to verify the signature generated with its

matching private key held by phone running the Microsoft Authenticator App or a Windows 10/11 device natively having Windows Hello. *Id*. Being part of an asymmetric key pair, the pubic key corresponds to a private key.

162. Altering a Windows Hello credential ID causes authentication to fail. Being FIDO certified, Windows Hello utilizes the WebAuthn protocol. Credential IDs within the WebAuthn protocol are in a tamper proof format unable to be subsequently altered because "all that would happen if an authenticator returns the wrong credential ID, or if an attacker intercepts and manipulates the credential ID, is that the WebAuthn Relying Party would not look up the correct credential public key with which to verify the returned signed authenticator data (a.k.a., assertion), and thus the interaction would end in an error." *Id*. As altering the device ID (i.e., Credential ID) causes authentication to fail, the credential ID is necessarily in a tamper proof format unable to be altered. "Passwordless authentication using the Authenticator app follows the same basic pattern as Windows Hello for Business." *See* **Exhibit 22**. Following the same pattern, altering the device ID caused to be stored on the phone by the Authenticator App should produce the same result of causing authentication to fail. As Microsoft controls the protocol utilized by its Identity Platform, including the inability to sync passkeys across devices, users wanting the benefit of biometric authentication via the Microsoft Authenticator App or Windows Hello have no choice but to store on their phone or Windows device a credential ID uniquely identifying the integrated device in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

163. As with the FIDO standards implemented by Windows Hello, the Microsoft Authenticator app utilizes a private key to sign a challenge. *Id*. Private keys are notoriously known secret decryption values. If the Authenticator App and Windows Hello have the private key, the

public key must be held by Microsoft's Identity Platform. By being part of a pair split between the authenticator and Microsoft's Identity Platform, the private key is a secret decryption value is in a tamper proof format unable to be subsequently altered. As Microsoft controls the protocol utilized by its Identity Platform, including the use of public/private key validation, users wanting the benefit of biometric authentication via the Microsoft Authenticator App or Windows Hello have no choice but to store on their phone or Windows device a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered.

164. Microsoft describes user authentication via the Authenticator App and Windows Hello as comprising receipt of proof-of-presence challenge completed when the user enters their biometrics. *Id*. Entering their biometric necessarily requires receiving scan data from a biometric scan. When the user completes the challenge the private key held by the phone or Windows device is unlocked. Determining if the user successfully completed challenge necessarily requires comparing the scan data to the biometric data to determine whether the scan data matches the biometric data.

165. As detailed by Microsoft, after the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *Id*. The Microsoft Authenticator App operates either on iOS or Android phones. As iOS and Android phones are cellular phones, often possessing Wi-Fi and Bluetooth capability, anything sent to Microsoft Identity Platform will be sent wirelessly – either via Wi-Fi, Bluetooth, or the cellular network. Laptops are common Windows devices having biometric capabilities and are often connected to the internet via Wi-Fi or using a mobile phone as a hotspot. Accordingly,

anything sent to Microsoft Identity Platform will be sent wirelessly via the laptop's Wi-Fi connection or connected phones cellular connection.

166. After the user has completed the biometric challenge, a signature is generated with the authenticator's private key and sent to Microsoft Identity Platform for verification. *Id.* As previously noted, password-less authentication using the Authenticator App follows the same basic pattern as FIDO certified Windows Hello. FIDO incorporates the WebAuthn Protocol. *See* **Exhibit 35**. Accordingly, the challenge sent to the Authenticator App is the equivalent of a FIDO server challenge sent to the Windows Hello authenticator with a WebAuthn authenticatorGetAssertion request. The response to the request, therefore, will contain a signature signed by the authenticator's private key and a credential ID (i.e., device ID) identifying which public key to use to verify the signature. *See* **Exhibit 34**. Upon receiving the response, the WebAuthn/FIDO server will use the device ID (i.e., credential ID) to locate the appropriate public key to verify the signature generated with the private key. *Id.* Accordingly, a FIDO/WebAuthn server within the Microsoft Identity Platform will authenticate a device ID (i.e., credential ID) sent in response to successful completion of a biometric challenge.

167. As detailed *supra*, upon successful completion of the biometric challenge, a device ID and signature is sent from the authenticator to Microsoft Identity Platform for authentication. The Microsoft Identity Platform utilizes OpenID Connect and Microsoft encourages developers to gain an understanding of the protocol and concepts to add authentication to applications. *See* **Exhibit 36**. Within the protocol, Microsoft identifies its identity platform as an "authorization server" managing "trust relationships" and issuing security tokens applications and APIs use for granting access (i.e. authorization) and authentication. *See* **Exhibit 27**. Accordingly, Microsoft describes its Identity Platform as a third party that operates as a trusted authority for authentication.

168. As noted supra, the FIDO server within the Microsoft Identity Platform uses a credential ID operating as a device ID to verify a signature generated with a private key bound to the identified device (i.e., authenticator). Such action is made possible by registering the credentials with an account and associating the account with the credential ID and credential public key. *See* **Exhibit 34**. Accordingly, the Microsoft Identity Platform maintains a listing of legitimate device IDs.

169. Authentication is provided by a FIDO sever incorporated into the Microsoft Identity Platform in conjunction with OpenID Connect Authentication Server that is also incorporated into the Microsoft Identity Platform. While OpenID Connect is a federation protocol, it is compatible and complementary with FIDO. "The value of a FIDO authentication capability is amplified by a federated system, where the federation system extends the benefits of a FIDO authentication to applications and services without requiring FIDO to be directly integrated with those applications." *See* **Exhibit 37**. When a federated system, such as OpenID Connect, is combined with FIDO, the OpenID Provider (OP) sends a FIDO server challenge to an authenticator which is returned as the FIDO Authentication response. *Id.*

170. FIDO incorporates the WebAuthn Protocol. Accordingly, the FIDO server challenge sent will a be WebAuthn authenticatorGetAssertion request. The response to the request received will contain a signature generated by the authenticator's private key and a credential ID. *See* **Exhibit 35**. Upon receiving the response, the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify the signature generated with the private key. *See* **Exhibit 34**. Accordingly, a FIDO/WebAuthn server incorporated into Microsoft Identity Platform will authenticate a device ID (i.e., credential ID). After validating the device ID, the

FIDO/WebAuthn portion of Identity Platform "redirects the user agent back to the Application Provider with an authentication assertion". *See* **Exhibit 37**.

171. As the Microsoft Identity Platform utilizes OpenID Connect, the authentication assertion will be an ID Token. The ID Token received from Microsoft's Identity platform enables access to an application. The ID Token is thus an access message provided by Microsoft operating as a third party trusted authority allowing access to an application. Should the user also require an access token to access further features of the application, such as files containing stored data, the ID token can be exchanged for an access token. *See* **Exhibit 27**.

172. Further, Microsoft Family enables parents to "designate the age limit for content [a family member] will have permission to access", such as apps and games. *See* **Exhibit 38**.

173. Further, Microsoft actively markets to and does business with clients in the financial services space and its Identity Services, including the use of its authenticators to complete a financial transaction.

174. Microsoft has induced infringement, and continues to induce infringement, of at least claims 1 and 2 of the 905 Patent in violation of 35 U.S.C. § 271 by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claim 15 by making Microsoft Identity available for integration with developer applications, providing the Microsoft Authentication Library, and a substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less

architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

175. Microsoft contributes to direct infringement of at least claims 1 and 2 of the 905 Patent in violation of 35 U.S.C. § 271© by providing use of its universal platform password-less architecture incorporating as authenticators Windows Hello preinstalled on Windows 10/11 computers and the Microsoft Authenticator App available for download and Microsoft Identity Platform for use by users to access resources offered by Microsoft, including applications, services, and subscriptions. Microsoft also induces infringement of claim 15 by making Microsoft Identity available for integration with developer applications, providing the Microsoft Authentication Library, and a substantial knowledge base teaching developers and business subscribing to Microsoft's Identity and Access Management services about the features, use and integration of their resources into the password-less architecture. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

176. Microsoft received actual notice of the 905 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 905 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 905 Patent.

177. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 905 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 905 Patent throughout the United States,

including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the Accused Products. Some examples of Microsoft promoting the use of the accused products are packaging Windows Hello with Windows 10/11 and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 954 Patent.

178. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 905 Patent, thereby specifically intending for and inducing its customers to infringe the 905 Patent through the customers' normal and customary use of the Accused Products.

179. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 905 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 905 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

180. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 905 Patent, including claim 1. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 905 Patent and how its products infringe that patent.

181. The infringing aspects of the Accused Products can be used only in a manner that infringes the 905 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

182. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 905 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.[]

183. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 905 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 905 Patent by Microsoft.

CLAIM 4
(Infringement of 042 Patent)

184. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

185. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 042 Patent.

186. Microsoft infringes at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271 with respect to the Accused Products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

187. For example, Microsoft directly infringes at least claim 1 of the 042 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating the Microsoft Identity Platform and Microsoft approved authenticators developed by itself and its

OEM partners. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

188. To be used with Microsoft's Identity Platform, an authenticator needs to have FIDO2 certification. *See* **Exhibit 19**. Accordingly, all authenticators used to practice the method have to meet the standards set by Microsoft and FIDO.

189. The claims include a controller placing within memory information that can only be accessed by a corresponding access key provided by an external application. Such memory is present in FIDO compliant authenticators. The FIDO CTAP specification incorporates the WebAuthn Specification. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id.* The credential ID uniquely identifies its public key credential source. *Id.* In addition to the credential ID, each public key credential source contains a "credential private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party. *Id.* Every FIDO compliant authenticator, therefore, will store within memory a credential comprising a private key of an asymmetric key pair and a credential ID uniquely identifying the private/public key pair to which the private key belongs.

190. The credentials stored within a compliant authenticator can only be accessed with the appropriate access key. "A public key credential can only be used for authentication with the same entity (as identified by the RP ID) it was registered with." *Id.* When generating a response, therefore, the authenticator will only retrieve credentials corresponding to the RP ID provided to it by the external FIDO server. *Id.* Therefore, the RP ID is an access key.

191. During a WebAuthn authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. The authenticatorGetAssertion request contains a relying party identifier (RP ID). *Id.* The authenticatorGetAssertion is called in response to a get request issued by the relying party attempting authentication. *Id.* The RP ID is provided by the relying party attempting authentication from an external authenticator. As an authenticator will only return credentials corresponding to the RP ID access key provided by the external relying party, the authenticator has the controller and memory necessary for minimal embodiment of a personal digital key ("PDK").

192. The FIDO standard requires all communications with BLE authenticators be encrypted. *Id.* FIDO compliant BLE capable authenticators, accordingly, include a receiver-decoder circuit ("RDC") enabling encrypted communications.

193. As noted above, FIDO compliant authenticators include the elements of minimal embodiment of a PDK. Windows Hello is a FIDO compliant authenticator and therefore a PC running Windows is an external PDK. Further, Bluetooth or other wireless pairing between a BLE capable Microsoft-compatible FIDO2 security key (i.e., authenticator) and a Windows PC necessarily requires a first wireless link between the devices to establish the pairing.

194. During an authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. Browsers, such as Microsoft Edge and Google Chrome, operating on Windows 11 forward the authenticatorGetAssertion to the external authenticator. *See* **Exhibit 39**. Windows supports use of BLE and NFC roaming authenticators with Edge and Chrome web browsers. Regardless of the web browser, Windows provides WebAuthn APIs enabling interactions with

authenticators to take place. *See* **Exhibit 35**. As such, Windows will connect with a roaming authenticator over BLE or NFC to forward to the authenticator the authenticatorGetAssertion request received via either the Edge or Chrome web browser.

195. Authentication is a service provided by a FIDO server incorporated into the Microsoft Identity Platform, and the credential ID is necessary for Microsoft's FIDO server to perform the authentication function. Upon receiving the response (i.e., enablement signal), the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify a signature generated with the private key held by the authenticator. *See* **Exhibit 34**. As the proper credential ID is needed for Microsoft's FIDO server to authenticate a user, and the credential ID is included within a response to a get request having the appropriate relying party ID received from the Microsoft's FIDO server, the response to the authenticatorGetAssertion request generated by the authenticator is an enablement signal enabling authentication by Microsoft's FIDO server. The authenticator, accordingly, generates an enablement signal enabling one or more of an application, a function and a service on a device associated with an external RDC.

196. The responsibility for sending responses received from an authenticator via BLE or NFC falls upon the WebAuthn Client. *Id.* Microsoft identifies its Edge Browser as the WebAuthn client. *See* **Exhibit 40**. Similarly, Google identifies its Chrome browser as a WebAuthn client by noting it supports the use of passkeys from mobile devices, including permitting the use of an Android phone as a roaming authenticator on Windows. *See* **Exhibit 41**. As such, Edge and Chrome will forward the enablement signal received from a roaming authenticator to Microsoft's FIDO server.

197. Microsoft has induced infringement, and continues to induce infringement, of at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271 by making Microsoft Identity

available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

198. Microsoft contributes to direct infringement of at least claim 1 of the 042 Patent in violation of 35 U.S.C. § 271(c) by making Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

199. Microsoft received actual notice of the 042 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 042 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 042 Patent.

200. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 042 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 042 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the accused products. Some examples of Microsoft promoting the use of the accused products are packaging Windows Hello with Windows 10/11 and public documents,

which serve no function other than to direct users of the Accused Products toward infringing the 042 Patent.

201. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 042 Patent, thereby specifically intending for and inducing its customers to infringe the 042 Patent through the customers' normal and customary use of the Accused Products.

202. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 042 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 042 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

203. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 042 Patent, including claim 1. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 042 Patent and how its products infringe that patent.

204. The infringing aspects of the Accused Products can be used only in a manner that infringes the 042 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

205. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 042 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

206. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 042 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 042 Patent by Microsoft.

CLAIM 5
(Infringement of 289 Patent)

207. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

208. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 289 Patent.

209. Microsoft infringes at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

210. For example, Microsoft directly infringes at least claims 14 and 16 of the 289 Patent by making, using (*e.g.*, performing/executing), selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating the Microsoft Identity Platform and Microsoft approved authenticators developed by itself and its OEM partners. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

211. To be used with Microsoft's Identity Platform, an authenticator needs to have FIDO2 certification. *See* **Exhibit 19**. Accordingly, all authenticators used to practice the method have to meet the standards set by Microsoft and FIDO.

212. The claims include a controller placing within memory information that can only be accessed by a corresponding access key provided by an external application. Such memory is present in FIDO compliant authenticators. The FIDO CTAP specification incorporates the WebAuthn Specification. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id.* The credential ID uniquely identifies its public key credential source. *Id.* In addition to the credential ID, each public key credential source contains a "credential private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party. *Id.* Every FIDO compliant authenticator, therefore, will store within memory a credential comprising a private key of an asymmetric key pair and a credential ID uniquely identifying the private/public key pair to which the private key belongs.

213. The credentials stored within a compliant authenticator can only be accessed with the appropriate access key. "A public key credential can only be used for authentication with the same entity (as identified by the RP ID) it was registered with." *Id.* When generating a response, therefore, the authenticator will only retrieve credentials corresponding to the RP ID provided to it by the external FIDO server. *Id*. Therefore, the RP ID is an access key.

214. During a WebAuthn authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. The authenticatorGetAssertion request contains a relying party identifier (RP ID). *Id.*

The authenticatorGetAssertion is called in response to a get request issued by the relying party attempting authentication. *Id.* The RP ID is provided by the relying party attempting authentication from an external authenticator. As an authenticator will only return credentials corresponding to the RP ID access key provided by the external relying party, the authenticator has the controller and memory necessary for minimal embodiment of a personal digital key ("PDK").

215. The FIDO standard requires all communications with BLE authenticators be encrypted. *Id.* FIDO compliant BLE capable authenticators, accordingly, include a receiver-decoder circuit ("RDC") enabling encrypted communications.

216. As noted above, FIDO compliant authenticators include the elements of minimal embodiment of a PDK. Windows Hello is a FIDO compliant authenticator and therefore a PC running Windows is an external PDK. Further, Bluetooth or other wireless pairing between a BLE capable Microsoft-compatible FIDO2 security key (i.e., authenticator) and a Windows PC necessarily requires a first wireless link between the devices to establish the pairing.

217. During an authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. Browsers, such as Microsoft Edge and Google Chrome, operating on Windows 11 forward the authenticatorGetAssertion to the external authenticator. *See* **Exhibit 39**. Windows supports use of BLE and NFC roaming authenticators with Edge and Chrome web browsers. Regardless of the web browser, Windows provides WebAuthn APIs enabling interactions with authenticators to take place. *See* **Exhibit 35**. As such, Windows will connect with a roaming authenticator over BLE or NFC to forward to the authenticator the authenticatorGetAssertion request received via either the Edge or Chrome web browser.

218. Authentication is a service provided by a FIDO server incorporated into the Microsoft Identity Platform, and the credential ID is necessary for Microsoft's FIDO server to perform the authentication function. Upon receiving the response (i.e., enablement singal), the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify a signature generated with the private key held by the authenticator. *See* **Exhibit 34**. As the proper credential ID is needed for Microsoft's FIDO server to authenticate a user, and the credential ID is70ncludeed within a response to a get request having the appropriate relying party ID received from the Microsoft's FIDO server, the response to the authenticatorGetAssertion request generated by the authenticator is an enablement signal enabling authentication by Microsoft's FIDO server. The authenticator, accordingly, generates an enablement signal enabling one or more of an application, a function and a service on a device associated with an external RDC.

219. The responsibility for sending responses received from an authenticator via BLE or NFC falls upon the WebAuthn Client. *Id.* Microsoft identifies its Edge Browser as the WebAuthn client. *See* **Exhibit 40**. Similarly, Google identifies its Chrome browser as a WebAuthn client by noting it supports the use of passkeys from mobile devices, including permitting the use of an Android phone as a roaming authenticator on Windows. *See* **Exhibit 41**. As such, Edge and Chrome will forward the enablement signal received from a roaming authenticator to Microsoft's FIDO server.

220. Microsoft has induced infringement, and continues to induce infringement, of at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271 by making Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

221. Microsoft contributes to direct infringement of at least claims 14 and 16 of the 289 Patent in violation of 35 U.S.C. § 271© by making Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

222. Microsoft received actual notice of the 289 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 289 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 289 Patent.

223. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 289 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 289 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the accused products. Some examples of Microsoft promoting the use of the accused products are packaging Windows Hello with Windows 10/11 and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 289 Patent.

224. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or

import the accused products, despite its knowledge of the 289 Patent, thereby specifically intending for and inducing its customers to infringe the 289 Patent through the customers' normal and customary use of the Accused Products.

225. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 289 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 289 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

226. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 289 Patent, including claim 14. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 289 Patent and how its products infringe that patent.

227. The infringing aspects of the Accused Products can be used only in a manner that infringes the 289 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

228. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 289 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

229. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 289 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283,

Proxense is entitled to a permanent injunction against further infringement of the 289 Patent by Microsoft.

CLAIM 6
(Infringement of 960 Patent)

230. Proxense repeats and realleges all preceding paragraphs, as if fully set forth herein.

231. Proxense has not licensed or otherwise authorized Microsoft to make, use, offer for sale, sell, or important any products that embody the inventions of the 960 Patent.

232. Microsoft infringes at least claims 14 and 16 of the 960 Patent in violation of 35 U.S.C. § 271 with respect to the accused products. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

233. For example, Microsoft directly infringes at least claims 14 and 16 selling access to, and/or offering to sell access to within the United States Microsoft's universal platform password-less architecture incorporating the Microsoft Identity Platform and Microsoft approved authenticators developed by itself and its OEM partners. Under the coordination of Microsoft Identity Platform, the authenticators perform/execute and provide, a method for verifying a user during authentication of the device.

234. To be used with Microsoft's Identity Platform, an authenticator needs to have FIDO2 certification. *See* **Exhibit 19**. Accordingly, all authenticators used to practice the method have to meet the standards set by Microsoft and FIDO.

235. The claims include a controller placing within memory information that can only be accessed by a corresponding access key provided by an external application. Such memory is

present in FIDO compliant authenticators. The FIDO CTAP specification incorporates the WebAuthn Specification. Under the WebAuthn specification, "compliant authenticators protect public key credentials." *See* **Exhibit 34**. A public key credential refers to a public key credential source, which includes a credential ID. *Id.* The credential ID uniquely identifies its public key credential source. *Id.* In addition to the credential ID, each public key credential source contains a "credential private key". *Id.* "The credential private key is bound to a particular authenticator" and part of an asymmetric key pair containing a public key returned to a relying party *Id*. Every FIDO compliant authenticator, therefore, will store within memory a credential comprising a private key of an asymmetric key pair and a credential ID uniquely identifying the private/public key pair to which the private key belongs.

236. The credentials stored within a compliant authenticator can only be accessed with the appropriate access key. "A public key credential can only be used for authentication with the same entity (as identified by the RP ID) it was registered with." *Id.* When generating a response, therefore, the authenticator will only retrieve credentials corresponding to the RP ID provided to it by the external FIDO server. *Id.* Therefore, the RP ID is an access key.

237. During a WebAuthn authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. The authenticatorGetAssertion request contains a relying party identifier (RP ID). *Id.* The authenticatorGetAssertion is called in response to a get request issued by the relying party attempting authentication. *Id.* The RP ID is provided by the relying party attempting authentication from an external authenticator. As an authenticator will only return credentials corresponding to the RP ID access key provided by the external relying party, the authenticator

has the controller and memory necessary for minimal embodiment of a personal digital key ("PDK").

238. The FIDO standard requires all communications with BLE authenticators be encrypted. *Id.* FIDO compliant BLE capable authenticators, accordingly, include a receiver-decoder circuit ("RDC") enabling encrypted communications.

239. As noted above, FIDO compliant authenticators include the elements of minimal embodiment of a PDK. Windows Hello is a FIDO compliant authenticator and therefore a PC running Windows is an external PDK. Further, Bluetooth or other wireless pairing between a BLE capable Microsoft-compatible FIDO2 security key (i.e., authenticator) and a Windows PC necessarily requires a first wireless link between the devices to establish the pairing.

240. During an authentication ceremony, an authenticator receives an "authenticatorGetAssertion" request to provide cryptographic proof of user authentication. *See* **Exhibit 35**. Browsers, such as Microsoft Edge and Google Chrome, operating on Windows 11 forward the authenticatorGetAssertion to the external authenticator. *See* **Exhibit 39**. Windows supports use of BLE and NFC roaming authenticators with Edge and Chrome web browsers. Regardless of the web browser, Windows provides WebAuthn APIs enabling interactions with authenticators to take place. *See* **Exhibit 35**. As such, Windows will connect with a roaming authenticator over BLE or NFC to forward to the authenticator the authenticatorGetAssertion request received via either the Edge or Chrome web browser.

241. Authentication is a service provided by a FIDO server incorporated into the Microsoft Identity Platform, and the credential ID is necessary for Microsoft's FIDO server to perform the authentication function. Upon receiving the response (i.e., enablement singal), the WebAuthn/FIDO server will use the credential ID to locate the appropriate public key to verify a

signature generated with the private key held by the authenticator. *See* **Exhibit 34**. As the proper credential ID is needed for Microsoft's FIDO server to authenticate a user, and the credential ID is included within a response to a get request having the appropriate relying party ID received from the Microsoft's FIDO server, the response to the authenticatorGetAssertion request generated by the authenticator is an enablement signal enabling authentication by Microsoft's FIDO server. The authenticator, accordingly, generates an enablement signal enabling one or more of an application, a function and a service on a device associated with an external RDC.

242. The responsibility for sending responses received from an authenticator via BLE or NFC falls upon the WebAuthn Client. *Id*. Microsoft identifies its Edge Browser as the WebAuthn client. *See* **Exhibit 40**. Similarly, Google identifies its Chrome browser as a WebAuthn client by noting it supports the use of passkeys from mobile devices, including permitting the use of an Android phone as a roaming authenticator on Windows. *See* **Exhibit 41**. As such, Edge and Chrome will forward the enablement signal received from a roaming authenticator to Microsoft's FIDO server.

243. Microsoft has induced infringement, and continues to induce infringement, of at least claims 14 and 16 of the 960 Patent in violation of 35 U.S.C. § 271 by making Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

244. Microsoft contributes to direct infringement of at least claims 14 and 16 of the 960 Patent in violation of 35 U.S.C. § 271(c) by making Microsoft Identity available for integration with developer applications and creating a knowledge base on how to do so. Proxense contends

each limitation is met literally, and, to the extent a limitation is not met literally, it is met under the doctrine of equivalents.

245. Microsoft received actual notice of the 960 Patent at least as early as July 29, 2016 when Proxense sent Microsoft correspondence attaching a copy of the 960 Patent. Microsoft performed and continues to perform the acts that constitute direct and/or indirect infringement, with knowledge or willful blindness to the acts that constitute direct and/or indirect infringement of the 960 Patent.

246. Since at least July 29, 2016, through its actions and continued actions, Microsoft has indirectly infringed and continues to indirectly infringe the 960 Patent in violation of 35 U.S.C. § 271(b). Microsoft has actively induced product makers, distributors, retailers, and/or end users of the accused products to directly infringe the 960 Patent throughout the United States, including within this Judicial District, by, among other things, advertising and promoting the use of the accused products on various websites and in marketing material, including providing and disseminating product descriptions, operating manuals, and other instructions on how to implement and configure the accused products. Some examples of Microsoft promoting the use of the accused products are packaging Windows Hello with Windows 10/11 and public documents, which serve no function other than to direct users of the Accused Products toward infringing the 960 Patent.

247. Microsoft does so knowingly and intending that its customers and end users will commit these infringing acts. Microsoft also continues to make, use, offer for sale, sell, and/or import the accused products, despite its knowledge of the 960 Patent, thereby specifically intending for and inducing its customers to infringe the 960 Patent through the customers' normal and customary use of the Accused Products.

248. In addition, Microsoft has indirectly infringed and continues to indirectly infringe the 960 Patent in violation of 35 U.S.C. § 271(c) by selling or offering to sell in the United States, or importing into the United States, the accused products with knowledge that they are especially designed or adapted to operate in a manner that infringes the 960 Patent and despite the fact that the infringing technology or aspects of the products are not a staple article of commerce suitable for substantial non-infringing use.

249. For example, Microsoft is aware that the technology described above included in the accused products enables the product to operate as described above and that such functionality infringes the 960 Patent, including claim 14. Microsoft continues to sell and offer to sell these products in the United States after receiving notice of the 960 Patent and how its products infringe that patent.

250. The infringing aspects of the Accused Products can be used only in a manner that infringes the 960 Patent and thus have no substantial non-infringing uses. The infringing aspects of those instrumentalities otherwise have no meaningful use, let alone any meaningful non-infringing use.

251. Proxense has been injured and seeks damages to adequately compensate it for Microsoft's infringement of the 960 Patent. Such damages should be no less than a reasonable royalty under 35 U.S.C. § 284.

252. Upon information and belief, Microsoft will continue to infringe (both directly and indirectly) the 960 Patent unless permanently enjoined by this Court. Pursuant to 35 U.S.C. § 283, Proxense is entitled to a permanent injunction against further infringement of the 960 Patent by Microsoft.

DEMAND FOR JURY TRIAL

Plaintiff hereby requests a jury trial of all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendant infringes one or more claims of each of the Patents-in-Suit;

b. Entry of judgment declaring that Defendant's infringement of the Patents-in-Suit is willful;

c. An order awarding damages sufficient to compensate Plaintiff for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding Plaintiff its costs and reasonable attorney fees pursuant to 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: April 28, 2023

Respectfully submitted,

/s/ David L. Hecht
David L. Hecht **(Co-Lead Counsel)**
dhecht@hechtpartners.com
Maxim Price *(pro hac vice forthcoming)*
mprice@hechtpartners.com
Conor B. McDonough *(pro hac vice forthcoming)*
cmcdonough@hechtpartners.com
Yi Wen Wu *(pro hac vice forthcoming)*
wwu@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
Bryce T. Barcelo
bbarcelo@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 *(pro hac vice forthcoming)*
ljiang@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067-6029
Telephone: (310) 789-3100
Facsimile: (3103) 789-3150

Counsel for Plaintiff Proxense, LLC

EXHIBIT 18

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

PROXENSE, LLC, *Plaintiff,*	§	
	§	**W-23-CV-00319-ADA**
v.	§	
MICROSOFT CORP, *Defendants.*	§	

Order

Before the Court are the parties' claim constructions briefs. Plaintiff Proxense, LLC filed its complaint for patent infringement on May 2, 2023. ECF No 1. Defendant Microsoft Corporation submitted the opening *Markman* Brief on November 11, 2023, and the Reply *Markman* Brief on December 11, 2023. ECF Nos. 31, 46, respectively. Proxense submitted its response on November 27, 2023, and its sur-reply brief on December 27, 2024. ECF Nos. 42, 49, respectively. The parties also submitted their Joint Claim Construction Statement on January 10, 2024. ECF No 51. The parties informed the Court that they would rest on their briefing in lieu of a *Markman* hearing. This Order informs the parties of the Court's final constructions of the disputed terms. Further, the Court **ADOPTS** the agreed constructions from the Joint Claim Construction Statement. ECF No. 51 at 2.

I. Legal Standard

Generally, courts construe claim terms according to their plain and ordinary meaning. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). The Federal Circuit applies a "heavy presumption" in favor of construing terms according to their plain and ordinary meaning,

that is, the "meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Azure Networks, LLC v. CSR PLC*, 771 F.3d 1336, 1347 (Fed. Cir. 2014) (vacated on other grounds); *Phillips*, 415 F.3d at 1313. The "only two exceptions to [the] general rule" that claim terms are construed according to their plain and ordinary meaning are when the patentee acts as his own lexicographer or disavows the full scope of the claim term either in the specification or during prosecution. *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). To act as his own lexicographer, the patentee must "clearly set forth a definition of the disputed claim term," and "clearly express an intent to define the term." Id. at 1365. To disavow the full scope of a claim term, the patentee's statements in the specification or prosecution history must represent "a clear disavowal of claim scope." Id. at 1366. Accordingly, when "an applicant's statements are amenable to multiple reasonable interpretations, they cannot be deemed clear and unmistakable." *3M Innovative Props. Co. v. Tredegar Corp.*, 725 F.3d 1315, 1326 (Fed. Cir. 2013). While the specification "may aid the court" in analyzing disputed language in a claim, "particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (internal citations omitted). Absent a "clear indication in the intrinsic record that the patentee intended the claims to be…limited," courts do not read limitations found in the specification into the claims. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 913 (Fed. Cir. 2004).

II. The Court's Constructions of Disputed Terms

Claim Term	Microsoft's Proposed Construction	Proxense's Proposed Construction	Court's Final Construction
"access message …" ('730 Patent claims 1, 15;	A message enabling acess	Adopt the Construction from *Proxense v. Samsung*, 6:21-cv-00210:	No construction necessary. Plain and ordinary meaning.

’954 Patent claim 1; ’905 Patent claim 1)		A signal or notification enabling or announcing access.	
“wherein the biometric data and the scan data are both based on a fingerprint scan by the user.” (’730 Patent, claim 5)	Indefinite or invalid under 35 U.S.C. § 112, ¶ 4	Adopt the Construction from *Proxense v. Samsung*, 6:21-cv-00210: Plain and ordinary meaning. No construction needed.	No construction necessary. Plain and ordinary meaning.
“receiver-decoder circuit” (’042 Patent, claim 10; ’289 Patent, claim 14)	A circuit that wirelessly receives encrypted data from the PDK and decodes it	Adopt the Construction from *Proxense v. Samsung*, 6:21-cv-00210: A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing.	A component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing
“personal digital key” (’042 Patent, claim 10)	A device that includes an antenna, a transceiver for communicating with the RDC and a controller and memory for storing	Adopt the Construction from *Proxense v. Samsung*, 6:21-cv-00210: An operably connected collection of elements	An operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user

	information particular to a user	including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.	

SIGNED this 24th Day of May, 2024.

ALAN D ALBRIGHT
UNITED STATES DISTRICT JUDGE

EXHIBIT 19

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANTS:	John J. Giobbi
APPLICATION NO.:	11/314,199
FILING DATE:	December 20, 2005
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO.:	10001-02090

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Eastern Time Zone of the United States on the local date shown below:

Dated: January 3, 2011 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT D

Sir/Madam:

Responsive to the Office Action mailed on November 22, 2010, which sets a shortened statutory period for response that expires on February 22, 2011, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below. Please amend claims 1, 10, 15 and 19 as indicated herein.

1. (Currently Amended) A method for verifying a user during authentication of an integrated device, comprising the steps of:

persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>; and

responsive to authentication of the code <u>by the agent</u>, receiving an access message from the agent, to allow user access.

2. (Previously Presented) The method of claim 1, wherein the code is transmitted to the agent over a network.

3. (Original) The method of claim 1, further comprising:
registering an age verification for the user in association with the code.

4. (Canceled).

5. (Original) The method of claim 1, wherein the code indicates that the biometric verification was successful.

6. (Canceled).

7. (Original) The method of claim 1, wherein the biometric data and the scan data are both based on a fingerprint scan by the user.

8. (Original) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the code for authentication.

9. (Original) The method of claim 1, further comprising:

receiving a request for the code without a request for biometric verification; and

responsive to receiving the request for the code without a request for biometric verification, sending the code without requesting the scan data.

10. (Currently Amended) An integrated device for verifying a user during authentication of the integrated device, comprising:

a persistent storage to store biometric data for a user and a code in a tamper-resistant format, the persistent storage being written once and being not altered subsequently, wherein the code uniquely identifies the integrated device;

a verification module, in communication with the persistent storage, to receive scan data from a biometric scan for comparison against the biometric data, and if the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices; and</u>

<u>a radio frequency communication module for receiving</u> ~~wherein responsive to authentication of the code, the agent transmits~~ an access message <u>from the</u>

agent that enables user access, responsive to the agent authenticating the code.

11. (Canceled).

12. (Previously Presented) The integrated device of claim 10, wherein the code is transmitted to the agent over a network.

13. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the code.

14. (Original) The integrated device of claim 10, wherein the verification module comprises:

an LED to be activated for requesting the biometric scan.

15. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving a code associated with a biometrically verified user, the code being registered with an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices;

requesting authentication of the code by the agent and the authentication determining whether the code is legitimate;

receiving an access message from the agent; and

in response to the access message being positive, providing access to an application.

16. (Canceled).

17. (Previously Presented) The method of claim 15, further comprising:

registering a date of birth or age with the agent.

18. (Original) The method of claim 15, further comprising:

establishing a secure communications channel with a biometric key, wherein the code associated with the biometrically verified user is received from the biometric key.

19. (Currently Amended) A system, comprising:

a biometric key to store biometric data for a user and a code in a tamper resistant format, and if scan data can be verified as being from the user by comparing the scan data to the biometric data, wirelessly sending the code, the code being associated with the verified user and uniquely identifying the biometric key; and

an authentication module to receive the code and send the code to agent for authentication to determine whether the code is legitimate, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>, and responsive to the code being authenticated, the <u>authentication module receiving from the agent</u> ~~agent sending~~ an access message to an application to allow the user to access the application.

20. (Original) The system of claim 19, wherein the biometric key receives an authentication request from the authentication module, and in response, requests a biometric scan from the user to generate the scan data.

21. (Original) The system of claim 19, wherein if the biometric key cannot verify the scan data as being from the user, it does not send the code.

22. (Previously Presented) The method of claim 1, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

23. (Previously Presented) The method of claim 15, wherein the application comprises one from a group of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site and a file.

24. (Previously Presented) The integrated device of claim 10, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

25. (Previously Presented) The system of claim 19, wherein the biometric data comprises one from a group of a palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition.

REMARKS

Claims 1-3, 5, 7-10, 12-15 and 17-25 were presented for examination. Claims 1-3, 5, 7-10, 12-15 and 17-25 stand rejected in the Office Action dated November 22, 2010 (herein, "OA"). Claims 1, 10, 15 and 19 are amended herein.

Response to Rejections Under 35 U.S.C. § 103

Claims 1-2, 5, 7-10, 12, 15, and 18-25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,041,410 A1 to Hsu et al. ("Hsu") in view of U.S. Patent Publication No. 2005/0074126 to Stanko ("Stanko"). This rejection is overcome in view of the amended claims.

As amended, independent claim 1 recites in part:

> persistently storing biometric data for the user and a code in a tamper-resistant format in a storage element on the integrated device that is written once and is not altered subsequently, wherein the code uniquely identifies the integrated device;
> responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;
> comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;
> responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority <u>including a list of codes identifying legitimate integrated devices</u>; and
> responsive to to authentication of the code <u>by the agent</u>, receiving an access message from the agent, to allow user access. (emphasis added)

The claimed invention beneficially allows multiple levels of authentication to determine user access. An integrated device persistently stores biometric data for a user and a code that uniquely identifies the integrated device in a storage element on the

integrated device. The code and biometric data are written once to the storage element and the storage element is not subsequently altered. Responsive to receiving a request for biometric verification of the user, the integrated device receives scan data from a biometric scan and compares the scan data to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, the code, which uniquely identifies the integrated device, is wirelessly transmitted to an agent that is a third party trusted authority including a list of codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code. Support for the amendment to claim 1 is found throughout the specification, for example at paragraphs [0038], [0039], [0042], [0043], [0049] and [0050].

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating the code uniquely identifying the integrated device, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the code, the claimed invention beneficially prevents unauthorized user of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "responsive to a determination that the scan data matches the biometric data, wirelessly

sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices."

Hsu merely discloses a system and method for verifying the identity of a person seeking to access a protected property. Hsu, 1:50-53. To verify identify, Hsu transmits data between a user's handheld device and a door. Hsu, Figure 1; 4:15-25. However, while the claimed invention determines that scan data matches biometric data then sends the code uniquely identifying the integrated device for authentication to a third-party trusted authority including a list of codes identifying legitimate integrated devices, Hsu at most transmits a cyclic redundancy code (CRC) from a portable device to a door. Hsu, 7:17-34. The transmitted CRC, however, identifies a reference fingerprint image and does not identify the user's handheld device. Hsu does not disclose any additional data, such as a code, that uniquely identifies an integrated device. As Hsu only discloses data identifying the reference fingerprint image and does not disclose or suggest a code uniquely identifying an integrated device, Hsu does not disclose "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Figure 4 and column 7, lines 20-30 of Hsu are cited in the OA and disclose:

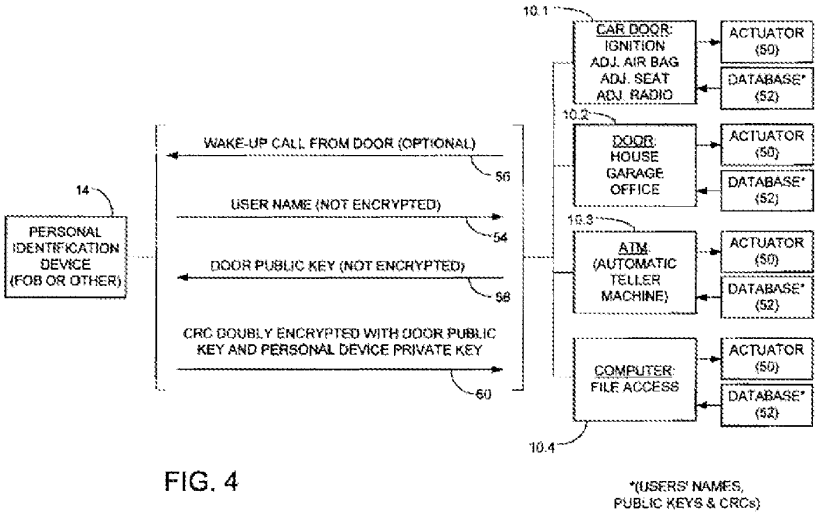


FIG. 4

without encryption, as indicated by line **58**. Then, if the fob **14** has validated the user's identification by successfully matching the sensed fingerprint image with the reference image, the fob performs two levels of encryption on the CRC that is generated. First, the encryption logic **34** in the fob **14** encrypts the CRC using the door's public key. Then the resulting encrypted CRC is doubly encrypted using the fob's private key. The doubly encrypted CRC is transmitted to the door **10**, where it is decrypted using the fob's public key and then using the door's private key to recover the CRC. The door **10** then compares this CRC with the CRC in

Hence, Figure 4 of Hsu merely discloses that the CRC is encrypted with the door's public key and the personal device's private key and the doubly-encrypted CRC is transmitted to the door. However, as depicted by Figure 4, the door does not include "a list of codes identifying legitimate integrated devices," but merely includes <u>user-specific</u> data such as names, public keys and CRCs. No device-specific data is maintained by the door, much less "a list of codes identifying legitimate integrated devices," as claimed. Similarly, column 7, lines 20-30 of Hsu disclose doubly encrypting the CRC and transmitting the doubly-encrypted CRC from the fob to the door. After decrypting the doubly-encrypted CRC, the door compares the CRC with stored CRCs. However, column 7, lines 20-30 of Hsu, and the remaining disclosure of Hsu, do not disclose or suggest that the door

includes "a list of codes identifying legitimate integrated devices," so there is consequently no disclosure of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

While the claimed invention both determines whether scan data matches persistently stored biometric data and authenticates a code uniquely identifying the integrated device using a third-party trusted authority including a list of codes identifying legitimate integrated devices, Hsu merely verifies whether a CRC identifying a fingerprint matches a stored CRC. Hence, Hsu merely verifies biometric data against two sources of stored biometric data and does not authenticate an integrated device by transmitting a code uniquely identifying the integrated device to an agent that "is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Stanko fails to remedy the deficient disclosure of Hsu. Rather, Stanko discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. However, Stanko merely redirects a ticket digitally signed using an authentication server's private key to a secure server that verifies the digital signature to allow access to the secure server. Stanko, ¶ [0055]. Stanko uses authentication of user credentials by one secure server to allow an authenticated user to access additional secure servers without retransmitting the user credentials. Stanko, ¶¶ [0048]-[0050]. Thus, Stanko uses a single set of user credentials for authentication and does not then transmit a code uniquely identifying an integrated device to a third-party

trusted authority including a list of codes identifying legitimate integrated devices responsive to scan data matching stored biometric data. Hence, Stanko also fails to disclose or suggest "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Accordingly, the cited references, both alone and in combination, fail to disclose at least the claimed element of "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices." Thus, claim 1 is patentably distinct from the cited references, and reconsideration and withdrawal of its rejection is respectfully requested.

As claims 2, 5, 7-9 and 22 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 5, 7-9 and 22. Therefore, claims 2, 5, 7-9 and 22 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 10, 15 and 19 are amended herein to recite similar elements as amended claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 10, 15 and 19. Accordingly, claims 10, 15 and 19 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claims 12 and 24 depend from claim 10, all arguments advanced above with respect to claim 1 are also applicable to claims 12 and 24. Similarly, claims 18 and 23

depend from claim 15, so all arguments advanced above with respect to claim 1 are also applicable to claims 17, 18 and 23. Also, claims 20 and 25 depend from claim 19, so all arguments advanced above with respect to claim 1 are also applicable to claims 20 and 25. Hence, claims 12, 18, 20 and 23-25 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 13, 14 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Hsu and Stanko further in view of U.S. Patent Publication No. 2004/0129787 A1 to Saito et al. ("Saito"). This rejection is overcome in view of the amended claims.

As claim 3 depends from claim 1, all arguments advance above with respect to claim 1 are hereby incorporated so as to apply to clam 3. As claims 13 and 14 depend from claim 10, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claims 13 and 14. As claim 17 depends from claim 15, all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to claim 17.

Saito fails to remedy the deficient disclosure of Hsu. Rather, Saito discloses a smartcard system for biometric identification. Saito, Abstract. Like Hsu, Saito merely matches captured biometric data against multiple sources and does not also authenticate an integrated device by transmitting a code uniquely identifying the integrated device to an agent that "is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed. Saito merely verifies that captured biometric data matches locally stored data and, if the captured biometric data matches locally stored

data, verifies that the captured biometric data matches data in a remote authentication system. Saito, ¶ [0008]. While Saito provides that the local match and remote match of the captured biometric data may be different, only biometric data is matched using the different systems. Saito, ¶ [0008]. There is no disclosure or suggestion in Saito of a code uniquely identifying the integrated device or of a trusted-third party authority including a list of codes identifying legitimate integrated devices. Hence, Saito also fails to disclose "responsive to a determination that the scan data matches the biometric data, wirelessly sending the code for authentication to an agent, wherein the agent is a third-party trusted authority including a list of codes identifying legitimate integrated devices," as claimed.

Thus, claims 3, 13, 14 and 17 are patentably distinct from the cited references, both alone and in combination, and reconsideration and withdrawal of their rejection is respectfully requested.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: January 3, 2011 By: /Brian G. Brannon/

Brian G. Brannon, Reg. No. 57,219
Attorney for Applicants
PATENT LAW WORKS LLP
165 South Main Street, Second Floor
Salt Lake City, UT 84111
Tel.: (801) 258-9838
Fax: (801) 355-0160
Email: bbrannon@patentlawworks.net

EXHIBIT 20

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

APPLICANT:	John J. Giobbi
APPLICATION NO:	13/710,109
FILING DATE:	December 10, 2012
TITLE:	Biometric Personal Data Key (PDK) Authentication
EXAMINER:	Phy Anh Tran Vu
GROUP ART UNIT:	2437
ATTY. DKT. NO:	10001-03653 US
CONFIRMATION NO:	5712

CERTIFICATE OF EFS-WEB TRANSMISSION

Pursuant to 240 OG 45 and the Legal Framework For EFS-Web, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Mountain Time Zone of the United States on the local date shown below:

Dated: September 13, 2013 By: /Matthew Holmes/
Matthew Holmes, Reg. No. 65,160

COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

AMENDMENT A

Sir/Madam:

Responsive to the Office Action mailed on June 13, 2013, which sets a shortened statutory period for response that expires on September 13, 2013, please enter the following amendment and consider the following remarks.

IN THE CLAIMS

All pending claims are reproduced below.

1. (Currently Amended) A method comprising:

persistently storing biometric data of [[the]]a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;

responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan;

comparing the scan data to the biometric data to determine whether the scan data matches the biometric data;

responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other values from the plurality of codes and [[the]]other data values for authentication by an agent that is a third-party trusted authority, wherein the one or more codes and other data values includes the device ID code; and

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

2. (Currently Amended) The method of claim 1, wherein the one or more codes and [[the]] other data values are transmitted to the agent over a network.

3. (Original) The method of claim 1, further comprising:

registering an age verification for the user in association with the device ID code.

4. (Currently Amended) The method of claim 1, wherein the one or more codes and [[the]]other data values indicate that the biometric verification was successful.

5. (Original) The method of claim 1, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

6. (Original) The method of claim 1, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

7. (Original) The method of claim 1, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

8. (Original) The method of claim 1, wherein the application includes a file including medical information.

9. (Original) The method of claim 1, wherein the application includes a financial account.

10. (Currently Amended) The method of claim 1, further comprising:

establishing a secure communication channel prior to sending the one or more codes and [[the]]other data values for authentication.

11. (Currently Amended) The method of claim 1, further comprising:

receiving a request for the one or more codes and [[the]]other data values without a request for biometric verification; and

responsive to receiving the request for the one or more codes and [[the]]other data values without a request for biometric verification, sending the one or more codes and [[the]]other data values without requesting the scan data.

12. (Currently Amended) An integrated device comprising:

a persistent storage [[to]]that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to the persistent storage and unable to be subsequently altered;

a verification module, coupled to communicate with the persistent storage, [[to]]that receives scan data from a biometric scan for comparison against the biometric data, and [[to]]that sends one or more codes and other data values from the plurality of codes and other data values for authentication by an agent, wherein the one or more codes and other data values includes the device ID code; and

a radio frequency communication module ~~for receiving~~ that receives an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

13. (Currently Amended) The integrated device of claim 12, wherein the one or more codes and [[the]]other data values are transmitted to the agent over a network.

14. (Original) The integrated device of claim 12, wherein an age verification is registered in association with the device ID code.

15. (Original) The integrated device of claim 12 comprising:

an LED to be activated for requesting the biometric scan.

16. (Currently Amended) A method for authenticating a verified user using a computer processor configured to execute method steps, comprising:

receiving one or more codes and other data values from a plurality of codes and other data values including a device ID code, wherein the plurality of codes and [[the]]other data values comprises the device ID code uniquely identifying an integrated device associated with a biometrically verified user, the device ID code being registered with an agent that is a third-party trusted authority;

requesting authentication of the one or more codes and [[the]]other data values by the agent;

receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values; and

in response to receiving the access message, allowing the biometrically verified user access to an application.

17. (Original) The method of claim 16, further comprising:

registering a date of birth or age with the agent.

18. (Currently Amended) The method of claim 16, further comprising:

establishing a secure communications channel with the integrated device, wherein the one or more codes and [[the]]other data values associated with the biometrically verified user is received from the integrated device.

19. (Original) The method of claim 16, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

20. (Original) The method of claim 16, wherein the application includes a file including medical information.

21. (Original) The method of claim 16, wherein the application includes a financial account.

22. (Currently Amended) A system, comprising:

an integrated device ~~for storing~~ that stores biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element in the integrated device that is unable to be subsequently altered, and [[for]]that wirelessly ~~sending~~ sends one or more codes and other data values from the plurality of codes and other data values, wherein the one or more codes and [[the]]other data values include the device ID code; and

an authentication unit ~~for receiving~~ that receives the one or more codes and [[the]]other data values and sends the one or more codes and [[the]]other data values to an agent for authentication, and ~~for receiving~~ that receives an access message from

the agent indicating that the agent successfully authenticated the one or more codes and other data values and allows the user to access an application.

23. (Currently Amended) The system of claim 22, wherein the integrated device receives an authentication request from the authentication unit, and in response, requests a biometric scan from the user to generate [[the]]scan data.

24. (Currently Amended) The system of claim 22, wherein when the integrated device cannot verify [[the]]scan data as being from the user, [[it]]<u>the integrated device</u> does not send the one or more codes and [[the]]other data values.

25. (Original) The system of claim 22, wherein the integrated device comprises one or more of a mobile phone, tablet, laptop, mp3 player, mobile gaming device, watch and a key fob.

26. (Original) The system of claim 22, wherein the biometric data includes one or more of a fingerprint, palm print, a retinal scan, an iris scan, a hand geometry, a facial recognition, a signature recognition and a voice recognition;

27. (Original) The system of claim 22, wherein the application includes one or more of a casino machine, a keyless lock, a garage door opener, an ATM machine, a hard drive, computer software, a web site, a file and a financial account.

28. (Original) The system of claim 22, wherein the application includes a file including medical information.

29. (Original) The system of claim 22, wherein the application includes a financial account.

REMARKS

Claims 1-29 were presented for examination. Claims 1-29 stand rejected in the Office Action dated June 13, 2013 (herein, "OA"). Claims 1, 2, 4, 10-13, 16, 18 and 22-24 amended. Claims 1-29 are pending upon entry of this amendment.

Summary of Office Action

1. Claims 15 and 16 are objected to for alleged informalities.

2. Claims 1-5, 7, 10-18, 22-24 and 26-27 are rejected on the ground of non-statutory obviousness-type double patenting as being allegedly unpatentable over claims 1-4, and 6-17 of U.S. Patent No. 8,352,730.

3. Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AlA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regards as the invention, or for pre-AlA the applicant regards as the invention.

4. Claims 1-2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,41, hereinafter "Hsu") Stanko (US Published App 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (US Published App 2002/0129262, hereinafter "Kutaragi").

5. Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

6. Claim 15 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (US Published App 2004/0129787, hereinafter "Saito").

7. Claims 16, 18-19, and 21 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,410, hereinafter "Hsu") and Stanko (US Published App 2005/0074126, hereinafter "Stanko").

8. Claim 17 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

The rejections are traversed herein.

Response to Objections

Claims 15 and 16 are objected to for alleged informalities.

With regard to claim 15, Applicant does not understand why "biometric scan" is objectionable and respectfully requests that the Examiner explain why "biometric scan" is objectionable.

With regard to claim 16, the Examiner appears to argue that line 5 should recite "comprise" rather than "comprises." It appears that recitation of "**the** other data values" has created ambiguity and confusion. "Plurality" modifies both the codes and other values (e.g. one code and one other data value, or two codes, or two other data values, etc.), so "the plurality … comprises the device ID code" is grammatically correct. This construction is supported by paragraph [0035], which teaches that, in one embodiment, "the code is a device ID." Similarly, "one or more" modifies both codes and other data values." Applicant has amended claim 16 and

the other claims to remove "the" where it precedes "other data values" in an attempt to remove the apparent confusion and ambiguity.

Response to Double Patenting Rejection

Claims 1-5, 7, 10-18, 22-24 and 26-27 are rejected on the ground of non-statutory double patenting as being allegedly unpatentable over claims 1-4 and 6-17 of U.S. Patent No. 8,352,730. Applicant does not acquiesce to the propriety of the double patenting rejection, but has submitted a terminal disclaimer with this amendment to advance prosecution. Accordingly, the Examiner is requested to withdraw the double patenting rejection.

Response to Rejections under 35 U.S.C. § 112

Claims 12-15 and 22-29 are rejected under 35 U.S.C. §112(b) or 35 U.S.C. §112 (pre-AlA), second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor regard as the invention, or for pre-AlA the applicant regards as the invention.

Claims 1 and 24 are amended to correct the antecedent bases indicated by the Examiner. Claims 12 and 22 are amended to remove the "to" and "for" language that the Examiner based the section 112 rejection upon. Therefore, Applicant respectfully requests that the Examiner withdraw the section 112 rejection and allow the claims.

Response to Rejections under 35 U.S.C. § 103

Claims 1-2, 4-7, 9-13, 22-27 and 29 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,41, hereinafter "Hsu") Stanko (US Published

App 2005/0074126, hereinafter "Stanko") and in view of Kutaragi et al. (US Published App 2002/0129262, hereinafter "Kutaragi").

As amended, independent claim 1 recites in part:

> persistently storing biometric data of a user and a plurality of codes and other data values comprising a device ID code uniquely identifying an integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;
> responsive to receiving a request for a biometric verification of the user, receiving scan data from a biometric scan; . . .
> responsive to a determination that the scan data matches the biometric data, wirelessly sending one or more codes and other data values from the plurality . . . wherein the one or more codes and other data values includes the device ID code; and
> receiving an access message from the agent indicating that the agent successfully authenticated the one or more codes and other data values and allowing the user access to an application.

The claimed invention beneficially allows multiple levels of authentication to determine user access. Biometric data of a user and a plurality of codes and other data values comprising a device ID uniquely identifying the integrated device and a secret decryption value are persistently stored in a storage element on the integrated device. The biometric data and plurality of codes and other data values are written to a storage element on the integrated device that is unable to be subsequently altered. Responsive to receiving a request for biometric verification of the user, scan data from a biometric scan is received and compared to the persistently stored biometric data to determine whether the scan data matches the persistently stored biometric data. In response to determining that the scan data matches the persistently stored biometric data, one or more of the plurality of codes and other data values, including a device ID code uniquely identifying the integrated device are wirelessly transmitted to an agent that is a third party trusted authority possessing a list of the device ID codes identifying legitimate integrated devices for authentication. The user is allowed access responsive to receipt of an access message from the agent that authenticates the code.

Hence, the claimed invention provides two levels of user authentication without requiring a user to memorize and provide multiple credentials, such as a password and a personal identification number, associated with the integrated device. Further, by both matching scanned biometric data with stored biometric data and authenticating based on one or more of the plurality of codes and other data values, the claimed invention provides additional security against use of a stolen or expired integrated device by an illegitimate user. By verifying both the received biometric data and the integrated device itself, using the one or more of the plurality of codes and other data values, the claimed invention beneficially prevents unauthorized use of the integrated device.

The cited references do not disclose or suggest at least the claimed element of "persistently storing biometric data of a user … in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." The Examiner argues, on pages 14-15 of the OA, argues that Hsu teaches "persistently storing biometric data … in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered." Specifically, the Examiner argues:

> persistently storing biometric data of the user and a plurality of codes and other data values a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered *(Figure 3, element 32, column 4, lines 15-25; column 7, lines 6-9, and 63-65); fob's public and private key pair, door's keying information, user's name, account number or other identifying information);*

Respectfully, the Examiner is incorrect. Hsu at most discloses "the device [of Hsu]… is highly resistant to reverse engineering … and other techniques for tampering" is not the same as "tamper proof" as "proof" by general definition indicates a greater degree of imperviousness

than "resistant." Moreover, even assuming a common definition of "highly resistant to tampering" and "tamper proof," Hsu does not suggest or disclose, among other things, that the format in which the information is stored is necessarily what makes the device of Hsu device highly resistant to tampering. For example, the high resistance to tampering may merely refer to the fact that the communications to/from the device of Hsu are encrypted thereby making it difficult to clone communications or reverse engineer the contents of the communication. Because Hsu fails to disclose or suggest that the format of the data stored on its device contributes to the device's high resistance to tampering, Hsu fails to disclose or suggest "persistently storing biometric data … in a tamper proof format… that is unable to be subsequently altered" as recited by claim 1.

Neither Stanko nor Kutaragi remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose storing biometric information in a tamper proof format. Applicant has search Kutaragi, and Kutaragi fails to mention biometrics, much less "persistently storing biometric data … in a tamper proof format." Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Moreover, the cited references fail to disclose or suggest "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered." The Applicant respectfully direct the Examiner to Hsu 5:19-21, which states:

> area **32**, as indicated by the broken line **40**. Enrollment is performed when the user first acquires the fob **14**, and is normally not repeated unless the fob is lost or damaged. For

Hence, Hsu discloses that biometric is **normally** not repeated unless the fob is lost or damaged. Hsu does not disclose or suggest, among other things, that enrollment is **unable** to be repeated absent the loss of or damage to the fob. Hsu discloses a common practice and not a feature/limitation of the fob. For example, the enrollment of Hsu may not **normally** be repeated unless the fob is lost or damaged because an individual's fingerprints remain relatively unchanged for long periods of time eliminating the desire to re-enroll and not because the person is unable to re-enroll biometric information. 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 further eliminating the potential for tampering.

Neither Stanko nor Kutaragi remedy the deficient disclosure of Hsu. Stanko discloses discloses generation of digital signatures using private keys to allow a secure server to grant access to a client. Stanko, ¶ [0016]. As Stanko fails to at least disclose an integrated device persistently storing biometric information, Stanko does not disclose "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered," as recited by claim 1. Kutaragi fails to disclose or suggest biometrics, much less "persistently storing biometric data … to a storage element on the integrated device that is unable to be subsequently altered," as recited by claim 1. Therefore, claim 1 is patentably distinct from the cited references for at least this reason, and allowance of claim 1 is requested.

Applicant's claim 1 is patentable over the cited references for additional reasons. Applicant's invention biometrically verifies the user prior to using a third-party trusted authority

to authenticate the integrated device (based on one or more codes and other data values including the device ID code), and, responsive to successful authentication by the agent, allows the user access to an application. The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent by the integrated device responsive to a successful biometric authentication occurring on the integrated device.

Hsu at most discloses biometrically verifying the user at the integrated device before generating and encrypting a CRC based on the biometric information. The CRC is used for authentication at a door. A door is not a third-party trusted authority. In other words, Hsu does not provide two level authentication because Hsu verifies biometric information only (encryption does not necessarily verify the integrated device itself) and access is allowed/disallowed by the "door" without using a third-party trusted authority. Applicant's integrated device verifies both biometric data and the integrated device itself, and requires authentication by a third-party trusted authority.

Stanko does not disclose or suggest verifying biometric data prior to verifying the integrated device. Stanko discloses that an authentication server receives credentials, which may include biometrics, and the authentication server verifies the received credentials. Stanko, therefore, does not disclose verifying an integrated device itself nor does Stanko disclose verifying biometric information prior to authenticating the integrated device itself at a third-party trusted authority.

Kutaragi fails to disclose a biometric, much less sending a device ID code after successful biometric verification.

The cited references whether taken alone or in combination fail to disclose or suggest among other things "allowing access to an application" responsive to the integrated device being authenticated by a third-party trusted authority using "one or more codes and other data values [including a] device ID code" sent responsive to a successful biometric authentication as recited by claim 1. Therefore, claim one is patentably distinct from the cited references and allowance of claim 1 is requested.

As claims 2, 4-7 and 9-11 depend from claim 1, all arguments advanced above with respect to claim 1 are also applicable to dependent claims 2, 4-7 and 9-11. Therefore, claims 2, 4-7 and 9-11 are also patentably distinct from the cited references and reconsideration and withdrawal of their rejection is respectfully requested.

Independent claims 12, 16 and 22 recite language similar to claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claims 12, 16 and 22. Accordingly, claims 12, 16 and 22 are also patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

As claim 13 depend from claim 12, claim 13 is patentable over the cited references for at least the same reasons as claim 12 as well as the additional limitations it recites. Similarly, claims 23-27 and 29 depend from claim 22, so claims 23-27 and 29 are patentable over the cited references for at least the same reasons as claim 22 as well as the additional limitations they recite. Hence, claims 1-2, 4-7, 9-13, 22-27 and 29 are patentably distinct from the cited references, whether alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested.

Claims 3, 8, 14, 20 and 28 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

Claims 3 and 8 depend from claim 1, so all arguments advanced above with respect to claim 1 are hereby incorporated so as to apply to clams 3 and 8. Claim 14 depends from claim 12, so all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 14. Claim 20 depends from claim 16, so all arguments advanced above with respect to claim 16 are hereby incorporated so as to apply to clam 20. Claim 28 depends from claim 22, so all arguments advanced above with respect to claim 22 are hereby incorporated so as to apply to clam 28. Therefore, claims 3, 8, 14, 20 and 28 are patentable over Hsu, Stanko and Kutaragi.

Schlotterbeck fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Schlotterbeck at most disclose that a patient ID holds information such as age. *See* Schlotterbeck, ¶[0057]. Therefore, the cited portions of Schlotterbeck fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Moreover, holding an age does not disclose age verification,; therefore, claims 3 and 14 are patentable over Schotterbeck for at least this reason. Accordingly, withdrawal of the rejection is respectfully requested.

Claim 15 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko, Kutaragi and further in view of Saito et al. (US Published App 2004/0129787, hereinafter "Saito").

As claim 15 depends from claim 12, all arguments advanced above with respect to claim 12 are hereby incorporated so as to apply to clam 15. Therefore, claim 15 is patentable over Hsu, Stanko and Kutaragi. Saito fails to correct the deficiencies of Hsu, Stanko and Kuaragi, and the Examiner does not argue that it does. The cited portions of Saito at most disclose that an LED provides visible feedback to the user. *See* Stanko, ¶[0041]. Therefore, the cited portions of Saito fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Accordingly, withdrawal of the rejection is respectfully requested.

Claims 16, 18-19, and 21 are rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu et al. (USPN 6,041,410, hereinafter "Hsu") and Stanko (US Published App 2005/0074126, hereinafter "Stanko").

As mentioned above, independent claim 16 recites language similar to claim 1. Hence, all arguments advanced above with respect to claim 1 are also applicable to independent claim 16. Accordingly, claim 16 is patentably distinct from the cited references, both alone and in combination, so reconsideration and withdrawal of their rejection is respectfully requested. Claims 18-19 and 21 depend from claim 16 and are, therefore, patentable for at least the same reasons in addition to the other patentable elements they recite. Therefore, claims 16, 18-19, and 21 are patentably distinct from the cited references and withdrawal of their rejection is respectfully requested.

Claim 17 is rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Hsu, Stanko and further in view of Schlotterbeck et al. (US Published App 2004/0128162, hereinafter "Schlotterbeck").

Claim 17 depends from claim 16, so all arguments advanced above with respect to claim 16 are hereby incorporated so as to apply to clam 17. Therefore, claim 17 is patentable over Hsu, Stanko and Kutaragi. As explained above, Schlotterbeck fail to correct the deficiencies of Hsu, Stanko and Kuaragi. Accordingly, withdrawal of the rejection is respectfully requested.

CONCLUSION

Allowance of all claims is requested. If the Examiner believes that direct contact with Applicant's attorney will advance the prosecution of this case, the Examiner is encouraged to contact the undersigned as indicated below.

Respectfully submitted,
JOHN J. GIOBBI

Dated: September 13, 2013 By: /Matthew Holmes/

Matthew Holmes, Reg. No. 65,160
Attorney for Applicant
PATENT LAW WORKS LLP
201 South Main Street, Suite 250
Salt Lake City, UT 84111
Tel.: (385) 232-7853
Fax: (801) 355-0160
Email: mholmes@patentlawworks.net