

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00333

U.S. Patent No. 11,475,105

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

I. CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES.....	1
A.	Real Party-in-Interest	1
B.	Related Matters.....	1
C.	Lead and Back-up Counsel and Service Information	2
III.	GROUND FOR STANDING.....	2
IV.	THE '105 PATENT.....	3
A.	Summary of the '105 patent.....	3
B.	Prosecution History	4
C.	Effective Filing Date	5
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	8
VI.	CLAIM CONSTRUCTION	9
A.	“restricted interface” (Claims 9-11, and 28-30).....	9
VII.	REQUESTED RELIEF.....	11
VIII.	OVERVIEW OF CHALLENGES	11
A.	Challenged Claims	11
B.	Statutory Grounds for Challenges.....	12
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE..	13
A.	Ground 1: Claims 1, 14, 18, 33 and 35 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng and Kodama.....	13
1.	Kesanupalli.....	13
2.	Cheng	15
3.	Kodama	18
4.	Combination of Kesanupalli, Cheng and Kodama	19
5.	Claim 1	23
6.	Claim 14.....	43
7.	Claims 18 and 33.....	43

8.	Claim 35	45
B.	Ground 2: Claims 9-11 and 28-30 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng, Kodama and in further view of Challenger.	47
1.	Challener	47
2.	Reasons to Combine Kesanupalli, Cheng, Kodama and Challenger	49
3.	Claim 9	52
4.	Claim 10	56
5.	Claim 11	57
6.	Claims 28-30	58
C.	Ground 3: Claims 1, 9-11, 14, 18, 28-30, 33 and 35 are obvious under 35 U.S.C. §103 over Jakobsson '351 and Kodama.	58
1.	Jakobsson '351 and Kodama	58
2.	Reasons to Combine Jakobsson '351 and Kodama	58
3.	Claim 1	61
4.	Claims 9-11	67
5.	Claim 14	68
6.	Claims 18, 28-30 and 33	69
7.	Claim 35	70
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	71
A.	The <i>Fintiv</i> factors favor institution.	71
B.	The Board should not deny under General Plastic	73
C.	<i>Advanced Bionics</i> Test Favors Institution.	73
XI.	CONCLUSION	74
XII.	CERTIFICATE OF WORD COUNT	75
	CERTIFICATE OF SERVICE	76

PETITIONER’S EXHIBIT LIST

January 19, 2023

APPL-1001	U.S. Patent No. 11,475,105 (“the ’105 patent”)
APPL-1002	Prosecution History of the ’105 patent
APPL-1003	Declaration of Dr. Patrick McDaniel
APPL-1004	<i>Curriculum Vitae</i> of Dr. Patrick McDaniel
APPL-1005	Priority Chain Applications
APPL-1006	U.S. Patent No. 8,799,666 (“Kesanupalli”)
APPL-1007	U.S. Patent No. 8,099,789 (“Challener”)
APPL-1008	U.S. Patent Publication No. 2004/0117636 (“Cheng”)
APPL-1009	U.S. Patent No. 9,652,629 (“Brown”)
APPL-1010	European Patent Application EP 2 079 023 A2 (“Kodama”)
APPL-1011	U.S. Patent 10,360,351 (“Jakobsson ’351”)
APPL-1012	Patrick McDaniel, <i>Authentication</i> , Handbook of Computer Networks, Volume 3, Part 2, pp. 570-580, John Wiley and Sons, 2008. Ed. Hossein Bidgoli.
APPL-1013	IBM Introducing Fingerprint Reader Into Laptop. Jack Germain. 2004 at https://www.technewsworld.com/story/ibm-introducing-fingerprint-reader-into-laptop-37017.html
APPL-1014	U.S. Patent Publication 2008/0059804 to Shah et al.
APPL-1015	Kerberos: An Authentication Service for Computer Networks. B. Clifford Neuman et al. 1994 at https://gost.isi.edu/publications/kerberos-neuman-tso.html
APPL-1016	ISO/IEC 11889-1:2009 Information technology Trusted Platform Module Part 1: Overview at https://www.iso.org/standard/50970.html
APPL-1017	TPM Main Part 3 Commands Specification Version 1.2 1 March 2011 at https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf
APPL-1018	RESERVED

APPL-1019	Computer Dictionary, Second Edition, entry “record” (1994)
APPL-1020	How to Restore Your Data After a Hard Drive Crash, Glenn Derene, Aug 4, 2011 at https://www.popularmechanics.com/technology/gadgets/how-to/a6819/how-to-restore-your-data-after-a-hard-drive-crash/
APPL-1021	Redline comparison of U.S. Patent No. 10,360,351 patent specification and the ’105 patent.
APPL-1022	U.S. Patent Application No. 2008/0104416 to Challenger et al. (“Challenger’s PG-PUB”)
APPL-1023	RFC2818, HTTP Over TLS (May 2000)
APPL-1024	https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf (retrieved Jan. 2, 2024)
APPL-1025	Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation, (June 21, 2022) (“Director Memo)
APPL-1026	Preliminary Constructions, <i>Carbyne Biometrics v. Apple Inc.</i> , WDTX-1:23-cv-00324 (December 11, 2023)
APPL-1027	United States District Courts—National Judicial Caseload Profile (September 30, 2023), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30 (retrieved Dec. 14, 2023)
APPL-1028	Scheduling Order, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (July 14, 2023)
APPL-1029	Plaintiff Carbyne Biometrics, LLC’s Preliminary Infringement Contentions, <i>Carbyne Biometrics v. Apple, Inc.</i> , 1:23-cv-00324 (June 21, 2023)

I. INTRODUCTION

U.S. Patent No. 11,475,105 (the “’105 patent”) relates to “Authentication Translation” where a request to access a resource and an authentication input is received, and in response, “a previously stored credential associated with the resource is accessed” and provided to the resource. APPL-1001, Title, Abstract. Apple Inc. (“Petitioner” or “Apple”) respectfully requests the Board review and cancel as unpatentable under 35 U.S.C. §103(a) claims 1, 9-11, 14, 18, 28-30, 33, and 35 (“Challenged Claims”) of the ’105 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Apple Inc.

B. Related Matters

Pursuant to 37 C.F.R. §42.8(b)(2), the ’105 patent is or was involved in the following matters, which may affect, or be affected by, this proceeding:

- *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (WDTX), filed March 24, 2023 (Pending) (“Parallel District Court Proceeding”)

Apple is not aware of any disclaimers, reexamination certificates or other IPR petitions addressing the ’105 patent; however, the following matter involved a related application and may affect this proceeding:

- *Samsung Electronics Co., Ltd. et al v. RightQuestion, LLC*, IPR2022-00244 (PTAB), filed December 1, 2021 (terminated July 26, 2022) (“Samsung ’696 Patent IPR”)

C. Lead and Back-up Counsel and Service Information

Lead Counsel

David W. O’Brien
HAYNES AND BOONE, LLP
2801 N. Harwood St. Suite 2300
Dallas, TX 75201

Phone: (512) 867-8457
Fax: (214) 200-0853
david.obrien.ipr@haynesboone.com
USPTO Reg. No. 40,107

Back-up Counsel

Kelly Gehrke Lyle
HAYNES AND BOONE, LLP
2801 N. Harwood St. Suite 2300
Dallas, TX 75201

Phone: (512) 867-8528
Fax: (214) 200-0853
kelly.lyle.ipr@haynesboone.com
USPTO Reg. No. 62,332

Hong Shi
HAYNES AND BOONE, LLP
2801 N. Harwood St. Suite 2300
Dallas, TX 75201

Phone: (512) 867-8440
Fax: (214) 200-0853
hong.shi.ipr@haynesboone.com
USPTO Reg. No. 69,009

Please address all correspondence to lead and back-up counsel. Petitioner consents to electronic service and asks Patent Owner to do the same.

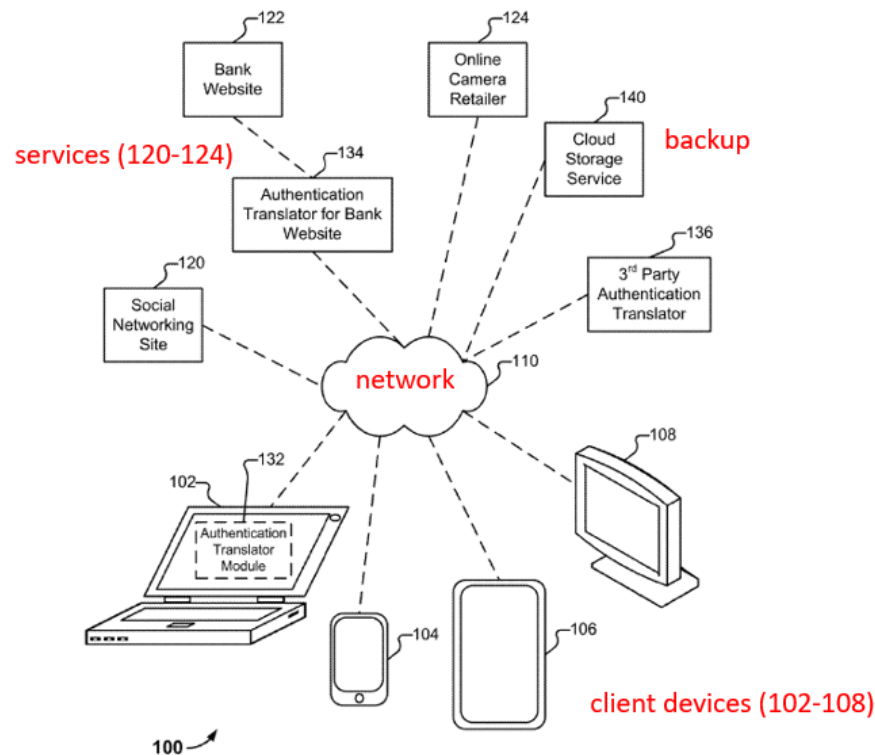
III. GROUNDS FOR STANDING

Petitioner certifies that the ’105 patent is eligible for IPR, and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

IV. THE '105 PATENT

A. Summary of the '105 patent

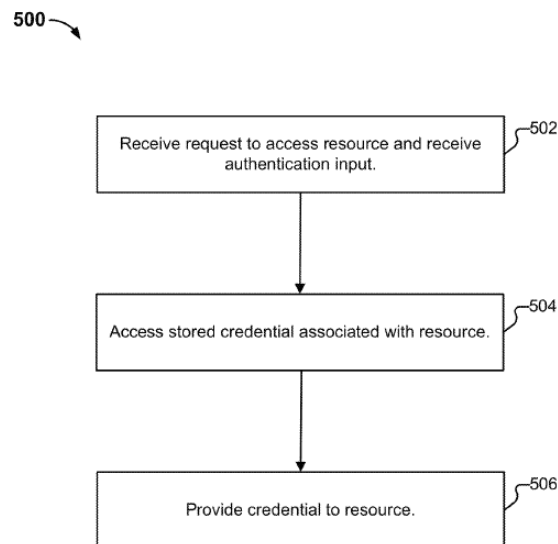
The '105 patent is directed to an environment including a client device, such as a notebook computer or tablet, which is connected via a network to a service such as a website. APPL-1001, 2:62-3:14. FIG. 1 is illustrative:



APPL-1001, FIG. 1, annotated

The '105 patent describes authentication techniques to provide user credentials (*e.g.*, a password) from a client device to a service with a goal of avoiding reliance on a user's input of the credential, which is tedious for the user and leads to poor security practices. APPL-1001, 1:43-52. The '105 patent

describes users “need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an ‘authentication translator’...and the authentication translator will provide the appropriate credentials to the implicated service on the user’s behalf.” APPL-1001, 3:20-26. FIG. 5 illustrates this authentication translation. APPL-1001, 1:66-67.



APPL-1001, FIG. 5

However, these techniques for authentication translation and the systems performing them were well-known at the time of the claimed invention. APPL-1003, ¶¶31-35.

B. Prosecution History

The Office rejected all claims as obvious but indicated that then-pending claim 16 reciting “the backup is performed in response to a determination that the

first device is of a same brand as the second device” was allowable. APPL-1002, 89-104 (Office Action dated 01-28-2022). The Office also rejected the claims on obviousness-type double-patenting grounds over various patents including U.S. Patent 10,360,351 (“Jakobsson ’351”). APPL-1002, 88-89. In a response with accompanying Terminal Disclaimer, Applicant amended each of its independent claims to require initiating backup to a second device is “based at least in part on the first device being a same brand as a second device.” APPL-1002, 69-70, 76-79. This also was well-known by the earliest claimed invention date. APPL-1003, ¶¶34-35.

C. Effective Filing Date

The ’105 Patent issued on a continuation-in-part (CIP) application (US Application 17/123,018 (“the ’018 App”)) filed December 15, 2020. APPL-1001, (22), (63); *see also* APPL-1002, 353-54 (ADS-Domestic Benefit), 397. The ’018 App claims priority as a CIP to U.S. Application 17/027,481, which claims priority through a chain of five (5) continuation applications originating with US Application 13/706,254 (“the pre-AIA ’254 App”), filed December 5, 2012. *Id.*

Applicable Law: Because the ’018 App was filed after March 16, 2013, but purports to claim benefit of a filing date before March 16, 2013, it is a “transition application.” The America Invents Act provides that its amendment of 35 U.S.C. §§102, 103 applies to “any application for patent, and to any patent issuing

thereon, that contains or contained at any time—(A) a claim to a claimed invention that has an effective filing date as defined in Section 100(i) of title 35, United States Code, that is [after March 15, 2013].” AIA §3(n)(1).

Here, the ’018 App contained (on filing) dependent claim 16, which contained the language “the backup is performed in response to a determination that the first device is of the same brand as the second device.” APPL-1002, 417. As confirmed by Dr. McDaniel, no disclosure exists in any application to which the ’018 App claims priority—including the pre-AIA ’254 App—that provides written description support for a backup being performed *in response to a determination* that the first device is *of the same brand* as the second device. APPL-1003, ¶¶36-41. Accordingly, AIA §3(n)(1) dictates the ’105 patent be evaluated under post-AIA §§102, 103.

Effective Filing Date: The claims are only entitled to the actual filing date of the ’018 App where description of the initiating a backup based at least in part on a first device being a same brand as a second device (a limitation of each claim) was first presented. APPL-1003, ¶¶36-41; APPL-1021 (redline ’105 patent specification and U.S. Patent 10,360,351 specification). For a claim in a later-filed application to be entitled to the filing date of an earlier application, the earlier application must provide written description support for the claimed subject matter. *Anascape, Ltd. v. Nintendo of Am. Inc.*, 601 F.3d 1333, 1337 (Fed. Cir. 2010). The

written description requirement “guards against the inventor’s overreaching by insisting that he recount his invention in such detail that his [or her] future claims can be determined to be encompassed within his original creation.” *Vas-Cath Inc. v. Mahurkar*, 935 F.2d 1555, 1561 (Fed. Cir. 1991). To satisfy the written description requirement, “the disclosure of the earlier application, the parent, must reasonably convey to one of skill in the art that the inventor possessed the later-claimed subject matter at the time the parent application was filed.” *Tronzo v. Biomet, Inc.*, 156 F.3d 1154, 1158 (Fed. Cir. 1998).

As confirmed by Dr. McDaniel, no written description exists in any application to which the ’018 App claims priority for initiating backup to a second device based at least in part on the first device ***being a same brand*** as a second device. APPL-1003, ¶¶36-41. To the extent passages of the ’018 App discuss the term “brand” (*i.e.*, those portions corresponding to 13:28-33 and/or 19:29-35 of the ’105 patent), these passages are not found in any application to which the ’018 App claims priority. APPL-1003, ¶¶39-41. These passages fall under a heading “ADDITIONAL EMBODIMENTS.” APPL-1001, 11:30; APPL-1002, 18. This heading begins a portion of the ’018 App’s specification that spans pages numbered 18 to 36; in contrast, the originally filed specification of the U.S. Application 17/027,481 of which the ’018 App is a CIP, does not include this heading and begins its claim recitation at its page 17. APPL-1002, 395-414;

APPL-1005, 38.

Accordingly, the effective filing date of each of the claims of the '105 patent is no earlier than December 15, 2020. For avoidance of doubt, only Ground 3 depends on this priority analysis.

V. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Here, Persons of Ordinary Skill in the Art (“POSITA”) at the time of the claimed invention¹ would have had a bachelor’s degree in an electrical engineering, computer engineering, computer science, or a related field, and at least two years of experience in the research, design, development, and/or testing of authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa. APPL-1003, ¶¶18-22. Furthermore, a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA. *Id.* However, Petitioner does not imply a person having an extraordinary level of skill should be regarded as POSITA.

¹ This discussion applies to POSITA both at the earliest claimed priority date (2011) and at the filing date of the '105 patent (2020).

VI. CLAIM CONSTRUCTION

During IPR, claims are construed according to the standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). 37 C.F.R. §42.100(b) (Nov. 13, 2018). The claims are construed to the extent necessary to resolve the underlying controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioner submits for purposes of this proceeding, and as set forth below, terms of the challenged claims should be given their plain and ordinary meaning. *Phillips*, 415 F.3d at 1314-17; APPL-1003, ¶¶62-64.

A. “restricted interface” (Claims 9-11 and 28-30)

A “*restricted interface*” is an interface that limits accessibility. APPL-1003, ¶¶63-64. As described above (*see* Section IV.C.), the ’105 patent issued on a CIP application that adds description beyond that appearing in the applications to which it claims priority including new disclosure providing examples of a “*restricted interface*.” *See* APPL-1001, 11:30-24:39 (“Additional Embodiments”).

Turning first to the original disclosure, the ’105 patent (like US 11,514,138, to which the ’105 patent claims priority as a CIP, and its parent US 10,929,512) describes an example device including “a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (*e.g.*, a camera or a fingerprint reader),” the specification refers to access limitations in the

device in connection with an application programming interface (API). APPL-1001, 4:29-33 (“users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API”). Thus, POSITA would understand *restricted interface* to at least include an API that limits accessibility to secure storage, a fingerprint sensor, or dedicated processor. APPL-1003, ¶63.

In addition to this originally described form of *restricted interface*, the ’105 patent adds examples including “dedicated physical connection from a processor permitted to access the secure storage,” such as “a bus” or secure storage “integrated with the processor” such as “a SoC (System on a Chip)” as well as forms of “an API (Application Programming Interface)” having limited accessibility. APPL-1001, 18:45-61 (added description in CIP).

In the Parallel District Court Proceeding and without differentiating between patents, Patent Owner proposed (and the court issued a preliminary construction) that the term *restricted interface* is to be understood in accord with plain and ordinary meaning. APPL-1026, 1. Nonetheless, Petitioner is mindful that, in review of a related patent, the term *restricted interface* was central to a non-institution decision that found another petitioner and its expert failed to explain how prior art teachings disclosed a “restricted interface” in part because no express construction was offered. *See* IPR2022-00251, Paper 17, 23, 25 (PTAB 2002).

Plain and ordinary meaning of “*restricted interface*” is an interface that limits accessibility. Petitioner also demonstrates in the following analysis that the prior art renders obvious a *restricted interface* including configurations explicitly described in the ’105 patent in hardware and API examples that limit accessibility to secure storage, a fingerprint sensor or a dedicated physical connection, which is included within the meaning of the term regardless of how it is construed.

VII. REQUESTED RELIEF

Petitioner asks the Board to institute trial and cancel the Challenged Claims.

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 1, 9-11, 14, 18, 28-30, 33 and 35 (“Challenged Claims”) of the ’105 patent are challenged.

B. Statutory Grounds² for Challenges

Grounds	Claim(s)	Basis
#1	1, 14, 18, 33, 35	§103 over Kesanupalli, Cheng and Kodama
#2	9-11, 28-30	§103 over Kesanupalli, Cheng and Kodama in further view of Challenger
#3	1, 9-11, 14, 18, 28-30, 33, 35	§103 over Jakobsson '351 and Kodama

Kesanupalli was filed March 24, 2010, published April 7, 2011, and issued August 5, 2014. Challenger was filed September 29, 2006, published May 1, 2008 (APPL-1022), and issued January 17, 2012. Cheng was filed September 24, 2003 and published June 17, 2004. Kodama published July 15, 2009. Kesanupalli and Challenger are prior art under at least §102(a)(2); Cheng and Kodama are prior art under at least §102(a)(1).

² As demonstrated above, the '105 patent is an AIA patent. *See supra*, Section VII.C; AIA § 3(n)(1). Were Patent Owner to contest that, it would be understood that Kesanupalli also qualifies as prior art under pre-AIA §§102(a), (e), Challenger (or Challenger's PG-PUB) also qualifies under pre-AIA §§102(a), (b), (e), and that Cheng and Kodama also qualify under pre-AIA §102(b).

Jakobsson '351 issued July 23, 2019 and qualifies as prior art under at least §102(a)(1). Only Ground 3 depends on the priority date of the Challenged Claims. *See* APPL-1003, ¶¶65-69.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1, 14, 18, 33 and 35 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng and Kodama.

1. Kesanupalli

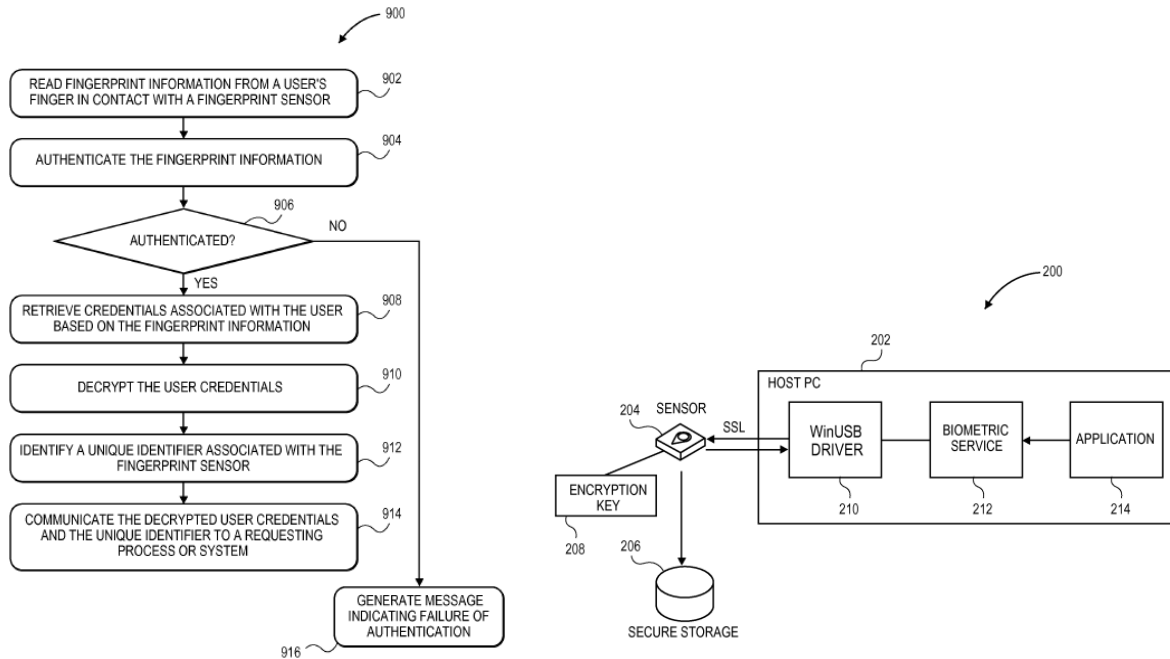
Kesanupalli is entitled “Secure User Authentication Using Biometric Information” and is directed to a secure authentication system using biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” APPL-1006, (54), 1:59-62. *See* APPL-1003, ¶¶70-75. Based on a match between a fingerprint template stored for a particular user and fingerprint information read from a finger presented at a fingerprint reader, Kesanupalli’s methods retrieve credentials associated with the user and communicate those credentials to an external system or process. APPL-1006, FIGS. 8-9, 3:14-4:11.

During an enrollment process with a resource such as a website, “a user swipes [or places] their finger [on] a fingerprint sensor several times to create [the] fingerprint template. The fingerprint template allows the user’s fingerprint to be distinguished from fingerprints associated with other users.” APPL-1006, 3:33-41. The user (or system) also “provides user credentials, such as a password,

cryptographic key...or the like,” and the systems and methods described in Kesanupalli “bind the user’s fingerprint template with the user credentials.” APPL-1006, 3:15-18, 3:41-46. To protect user credentials, “[t]he fingerprint template and user credentials are then stored in a secure storage of the user’s device.” APPL-1006, 3:46-47, *see also*, APPL-1006, 8:29-53.

During a subsequent user identification or verification for the website, a user presents her biometric information (*e.g.*, places a finger on a fingerprint sensor) and if the presented fingerprint “matches a fingerprint template, the user’s credentials are released to the user and/or [the] service or process requesting the user verification.” APPL-1006, 3:52-61. “[T]he user credentials released after finding a matching fingerprint template may include an OTP (One Time Password) token, RSA signature and the like,” such as a “cryptographic key.” APPL-1006, 3:41-44, 3:65-4:1, FIG. 12.

FIG. 9 of Kesanupalli illustrates these steps of authenticating a user in the context of an embodiment in which user credentials are cryptographically secured in storage. FIG. 2 illustrates an example system 200 in which user enrollment and authentication processes are performed using a biometric sensor 204, secure storage 206 and a Host PC 202. APPL-1006, 6:26-49, 9:10-24.



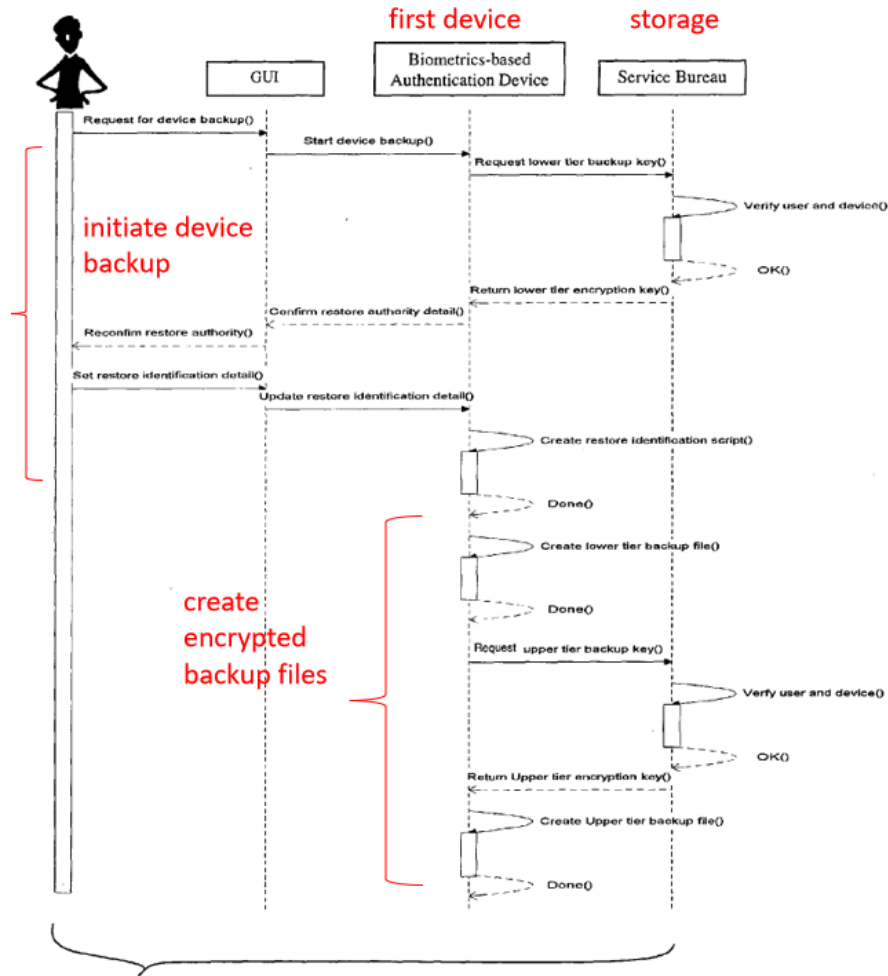
APPL-1006, FIGS. 9 and 2

In an authentication process, sensor 204 receives a biometric input from a user and releases the user's credentials from secure storage 206 upon a successful match of the input with the user's stored biometric template. APPL-1006, 6:31-45. The released credentials are then communicated to the external resource by an application 214 of the Host PC 202. APPL-1006, 5:9-58, 6:11-31.

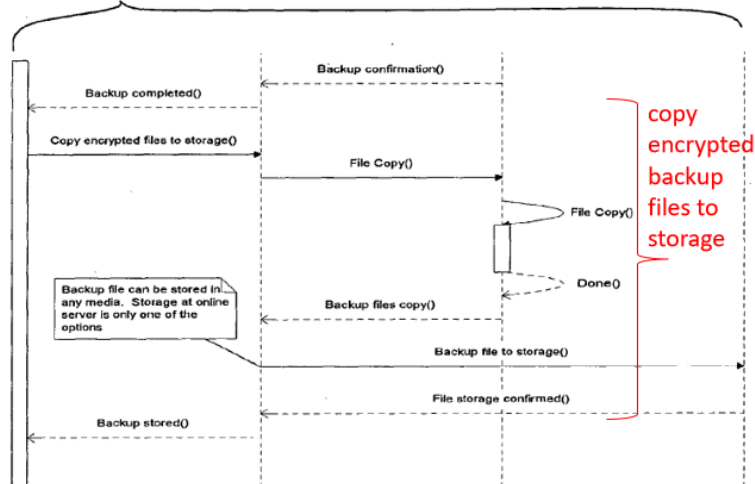
2. Cheng

Cheng is entitled "System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information" and provides ways to "securely backup and restore" a user's authentication-based device without compromising the security thereof. APPL-1008, (54), Abstract.

Cheng recognizes because “[b]iometrics-based authentication” is commonly implemented portable devices include “user’s authentication information, electronic identity and any data associated therewith.” APPL-1008, [0004], [0006]. Cheng securely backs-up this data to avoid costs of creating the data on new device from scratch should a first device containing the data be lost or stolen. *See* APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng’s FIGS. 3A-3B where a backup of a first user’s device data is performed through secure communication between a user service bureau (a storage service) and the device. APPL-1008, [0029]-[0030]. Cheng’s backup process includes a two-tier encryption procedure. APPL-1008, [0031]-[0039].



to FIG. 3B
from FIG. 3A



APPL-1008, FIG. 3A – 3B (portion), annotated

See APPL-1003, ¶¶76-79. Cheng describes a use case of a user's first device, having been backed up, becoming unavailable. A second device connects to the user service to download the data. APPL-1008, [0044]–[0050], FIGS. 4A-4C.

3. Kodama

Kodama is also directed to backing up data in an electronic device. APPL-1010, (57), [0040], [0041]. While Kodama centers around examples applying to a hard disk device (HDD), Kodama explains that its teachings are “not limited to an HDD recorder” and “can be applied to any electronic appliance such as a mobile phone, a PDA or a PC” and “there is no particular limitation in the backup target data upon applying the present invention.” APPL-1010, [0040], [0041].

Like Cheng, Kodama teaches registering a first device with a backup service (storage). APPL-1010, [0101]. Kodama's registration includes providing “device information including the manufacturer name.” *Id.* Kodama continues to describe sending data of the registered first device to the backup service. See APPL-1010, [0106]–[0107].

Kodama explains previously stored data of the backup service is restored onto another device (*e.g.*, a “new” device) and to start the restoration process “device information including the manufacturer name” of the second device is sent to the backup service system. APPL-1010, [0135]–[0136]. The backup service system verifies this new device information—including the manufacturer name—

coincides with the first device before permitting the backup of data to the new device. *See* APPL-1010, [0137-[0144]. *See also*, APPL-1003, ¶¶80-82.

4. Combination of Kesanupalli, Cheng and Kodama

POSITA would have been motivated to apply Cheng’s data backup teachings to Kesanupalli’s device including biometric information and credentials for user authentication. APPL-1003, ¶¶83-92. Kesanupalli’s device and its stored biometric information and credentials, which are a user’s personal data, combined with Cheng’s data backup teachings would produce obvious, beneficial, and predictable results of reducing the need to recreate the user’s personal data when using a new device (*e.g.*, a device replacing one having been lost or stolen). *Id.* POSITA would have been further motivated to apply Kodama’s teachings of ensuring devices implementing the backup are the same brand, which provides the obvious, beneficial, and predictable result of mitigating compatibility and security issues. *Id.*

Kesanupalli, Cheng, Kodama and the ’105 patent, are all in the same field of endeavor—security arrangements and procedures for protecting data in computer systems. APPL-1003, ¶85; *see, e.g.*, APPL-1006, 30-38 (“[S]ystems and methods described herein relate to biometric authentication of users...biometric information provides an additional level of security when used in systems and procedures related to authentication of a user.”), 2:48-50 (“client device, such as a

computer, cellular phone, and so forth”); APPL-1008, [0003], [0004] (“computers, electronics, communications, networks, and the Internet, access control in general and network security in particular have come increasingly important...To satisfy different security needs, various authentication systems, methods, and devices exist today and new ones are continually being developed.”); APPL-1001, 1:43-50 (“Providing credentials to a service, whether via a mobile or other device, is often a tedious experience for a user...[U]sers will often engage in practices...which render their credentials less secure against attacks. Accordingly, improvements in authentication techniques would be desirable.”), FIG. 1; APPL-1010, (57) (“The risk of a third party referring to or using back-up data without authorization upon restoring such backup data in an HDD recorder is mitigated”), [0040] (“The backup target application is not limited to an HDD recorder, and...can be applied to any electronic appliance such as a mobile phone, a PDA or a PC...”), [0041].

Moreover, as evidenced on the front pages of Kesanupalli, the ’105 patent, and Kodama, international, U.S. and/or the field of search classifications consulted by the Office during examination for each patent include the same subclass: CPC/IPC G0F6 21 (security arrangements for protecting computers, components thereof, programs or data against unauthorized activity). *See* APPL-1001, (51),

(52); APPL-1006, (51) (58); APPL-1010, (51).³ Cheng does not list a classification; however, POSITA would recognize it is directed to the same technology. APPL-1003, ¶86; APPL-1008, [0007] (“Enabling technologies include biometrics, authentication, cryptography, and encryption/ decryption.”)

Second, POSITA would have been motivated to employ Cheng’s backup technique in connection with Kesanupalli’s secure user authentication methods because Kesanupalli’s stored biometric information and credentials are personal data. APPL-1003, ¶¶87-91. POSITA would have understood stored personal data (biometric information and credentials) would need to be created and registered from scratch should the device be lost or stolen. *Id.*; APPL-1008, [0006]. Such a problem of inconvenience would have also been reasonably pertinent to the inventor of the challenged patent. *See* APPL-1001, 8:55-58. Thus, not only were Kesanupalli, Cheng/Kodama and the ’105 patent in the same field of endeavor, but Cheng would have been reasonably pertinent to a problem faced by the inventor of the ’105 patent as well as pertinent to known risks of theft and loss of devices and

³ *see also* www.uspto.gov/web/patents/classification/cpc/html/cpc-

[G06F.html#G06F](http://www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F) (subclass definitions);

www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (CPC to IPC concordance).

recovery of data that would have motivated POSITA to address by combining Cheng with Kesanupalli.

POSITA would readily recognize a personal electronic device can be lost, damaged, or otherwise require replacement. APPL-1003, ¶¶87-91; *see* APPL-1006, 10:13-18; APPL-1008, [0006]. And when introducing replacement devices, it is desirable to have access to the personal data without having to create the data from scratch. APPL-1008, [0006]-[0007]. Moreover, POSITA would have recognized a desire in the market of electronic devices to be capable of being backed up long before the '105 patent. APPL-1003, ¶89, APPL-1020. Cheng provides a benefit of implementing its techniques to perform the desired backup of personal data giving access to data in other user devices in a “reliable and secure way.” *Id.* In particular, Cheng teaches backing up personal data related to biometric information and secret keys. APPL-1008, [0007]–[0009]. This is data the same data as stored in Kesanupalli’s device. APPL-1006, 3:32-51.

Considering Kesanupalli’s device having Cheng’s backup technique, POSITA would have had further reason to employ Kodama’s technique of controlling backup processes such that the first device and the second device (that targeted to receive the data from the backup) are compatible. APPL, 1003, ¶84. Kodama recognizes “if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of data

between the products will differ.” APPL-1010, [0157], [0158]. POSITA would recognize benefits of transfer of data between like brands, including ensuring sufficient security protections for receipt and storage of personal data without introducing risk of compatibility issues. APPL-1003, ¶91.

Finally, POSITA would have had reasonable expectations of success in adding backup feature such as taught by Cheng as enhanced by Kodama in a biometric authentication system as taught by Kesanupalli because Cheng and Kodama are similarly directed to handling of personal information including biometric authentication information in a secure manner. APPL-1003, ¶92. Adding a backup feature would merely have been applying a known technique to a known device (method, or product) that is ready for improvement to yield predictable results. Backup features are implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli’s system and devices. *Id.* And enhancement of the backup feature according to Kodama is but a small addition of a brand check and supporting data to that routine software. *Id.*

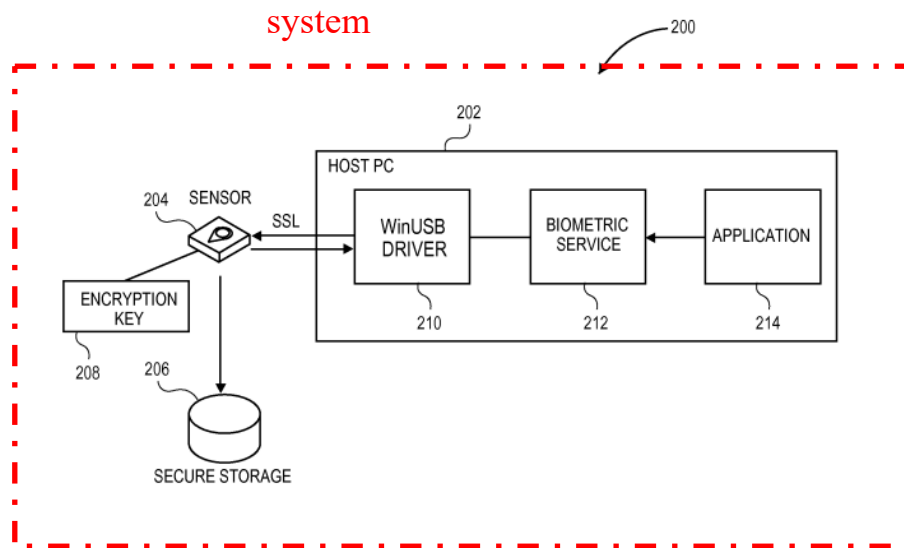
5. Claim 1

[1.0] *A system, comprising:*⁴

⁴ All emphasis in quoted material has been added. Claim terms are italicized.

Kesanupalli discloses *a system*. APPL-1003, ¶¶93-95.

Kesanupalli's FIG. 2 describes a system 200 "capable of performing biometric user enrollment and authentication." APPL-1006, 2:1-2. *See also*, APPL-1006, Abstract, FIGS. 11-12.



APPL-1006, FIG. 2, annotated

In Kesanupalli's system 200, sensor 204, including its secure storage 206, provides authentication translation and communicates with Host PC 202, which provides communication with external web servers including the communication of the user credential to website. APPL-1006, 6:11-49, FIG. 12.

Thus, Kesanupalli discloses *a system*, as claimed.

[1.1] *one or more processors configured to:*

Kesanupalli discloses or renders obvious *one or more processors* that are configured to perform the actions of claim 1 as described below. APPL-1003, ¶¶96-99.

Kesanupalli describes what POSITA would readily recognize—namely that functions of authentication translation and communication with external resources such as discussed in Section IX.A.1 and detailed below are performed by *one or more processors*. *Id*; APPL-1006, 9:58–10:1 (“The invention may also involve a number of **functions to be performed by a computer processor**, such as a microprocessor. The microprocessor may be a **specialized or dedicated microprocessor** that is configured to perform particular tasks according to the invention...”) The processor functions of authentication (*e.g.*, those of sensor 204 such as matching) and the processor functions of communicating with an external resource (*e.g.*, those of HOST PC 202) together provide *one or more processors*. *See id.*, APPL-1006, 5:62-6:31, 6:40-49.

Thus, Kesanupalli discloses *one or more processors*.

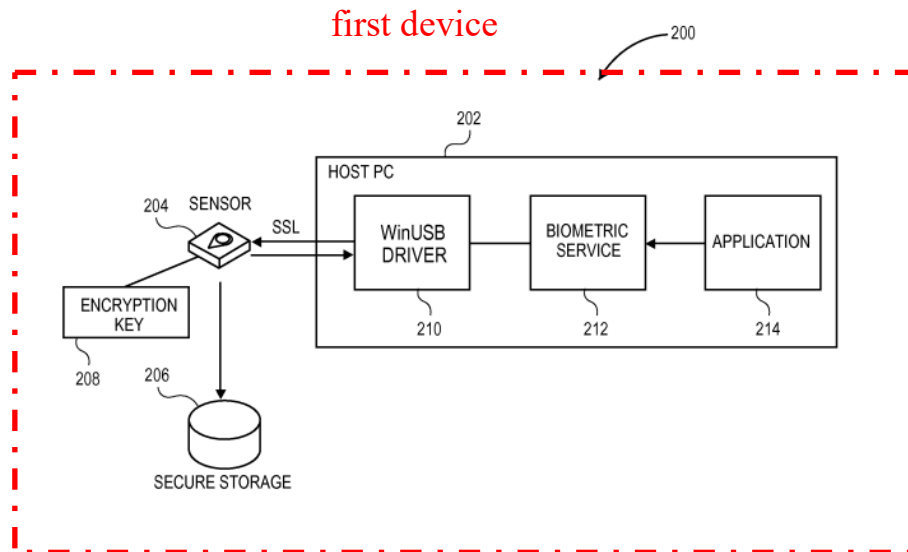
[1.2] *receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;*

Kesanupalli discloses this limitation. APPL-1003, ¶¶100-108.

As discussed above, Kesanupalli describes its functions are performed by one or more processors, which includes the functionality described with reference

to limitation [1.2].

Kesanupalli describes *a first device* exemplified in a first user device realization of FIG. 2. APPL-1003, ¶¶102-104.

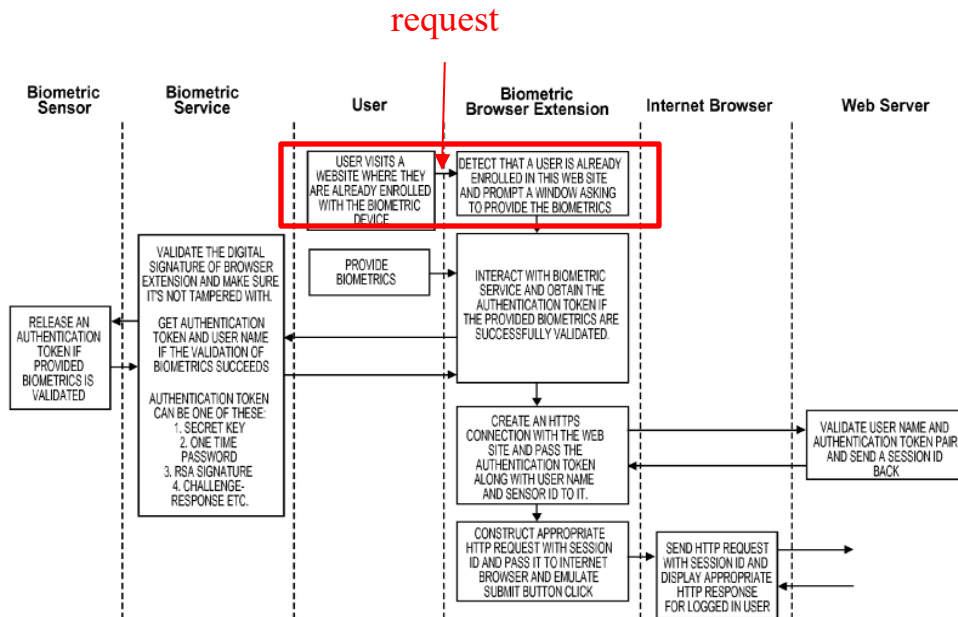


APPL-1006, FIG. 2, annotated

Biometric sensor 204, its secure storage 206, and Host PC 202 (including web browser application executing thereon) constitute *a device* that provides authentication translation and ultimately communicates user credentials to web servers. APPL-1006, Abstract, 2:54-3:3, 4:3-50, 6:11-49. Kesanupalli's embodiments (*e.g.*, FIG. 2) constitute a *device*, generically defined in claim 1 and the '105 patent. APPL-1003, ¶¶102-104; APPL-1001, 2:21-23. To the extent Patent Owner imparts some integrally-formed meaning for *device*, POSITA would understand Kesanupalli to disclose integrally-formed realizations of *a device*.

APPL-1003, ¶104; APPL-1006, 2:48-50 (“In particular embodiments, the biometric sensor is **physically attached (or manufactured into) a client device** such as a computer, cellular phone, and so forth. which also includes the sensor 204”), 3:48-51 (“In one embodiment the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.”)

Kesanupalli describes processor(s) *receiv[ing]*, at Host PC 202 of the first device, *a request* (visit to a website by user of PC 202) *to access a resource* (website) *external to the first device*. APPL-1006, 5:9-14 (“After a user has enrolled with a particular Web site that supports biometric authentication, **subsequent visits to the same Web site** cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication (*e.g.*, using the biometric device).”) *See also*, APPL-1006, 2:54-3:3, FIGS. 10-11. A user accessing/visiting a website in which she has enrolled means the user has made a *request* to access the site. APPL-1003, ¶105.



APPL-1006, FIG. 12, annotated

The request to access the resource is received by the processor of PC 202. APPL-1006, FIG. 2, 6:11-31.

The website visited by the user is *a resource external to the first device* as it is provided on a web server external to the first device. APPL-1006, 6:11-25, FIG. 12. And the website is *a resource associated with a user* as the user has visited the resource and previously enrolled. *See, e.g.*, APPL-1006, FIGS. 7, 11, 3:32-51.

Thus, Kesanupalli discloses this limitation.

[1.3a] access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access,

Kesanupalli discloses this limitation. APPL-1003, ¶¶109-118.

Again Kesanupalli's functions are performed by one or more processors, which includes the functionality described in limitation [1.3a].

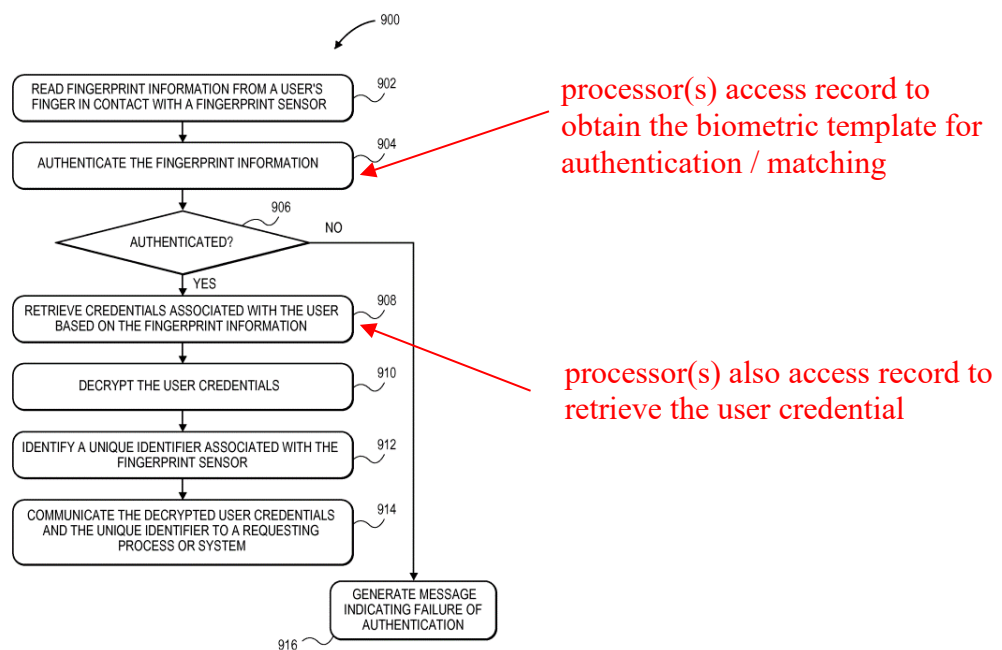
Kesanupalli describes a user's enrollment process in an external resource such as a website where the user's credential (key) and biometric template (fingerprint template) associated with the user and the website are stored in the first device (in secure storage 206). APPL-1006, 3:32-51 ("Initially, a user enrolls with the biometric user authentication system by **binding their user credentials with the user's biometric template (a 'fingerprint template' in specific implementations)**...During an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template...After creating a fingerprint template, the user (or a web server or other system) provides **user credentials**, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein **bind the user's fingerprint template with the user credentials**. The fingerprint template and user credentials are then stored in a **secure storage device**.") Kesanupalli in FIG. 7 walks through this enrollment process. APPL-1006, 8:29-53 (including block 710 where "the procedure binds

the user credentials with the fingerprint template[], then stores the user credentials and the fingerprint template [] in a secure storage.”). Authentication and “credentials” are known technologies in place long before the ’105 patent. APPL-1003, ¶¶43-57.

The user’s credential bound with a biometric template is a *record*, which is *stored on the first device* in a secure storage. APPL-1003, ¶¶113-114, citing APPL-1019 definition of record. Kesanupalli’s user credential is *credential information associated with the external resource (website) to which the user has requested access*. APPL-1006, 4:36-5:43 (including “...different user credentials are **associated with each Web site** with which the user enrolls.”). And Kesanupalli’s biometric template (fingerprint template) is *authentication information associated with the user* as it is the user’s personal biometric data. APPL-1003, ¶112.

After enrollment including creating and storing the record, user’s subsequent visits to the external resource initiate an authentication procedure. APPL-1006, 5:9-14 (“After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits cause...the Web site [to] prompt[] the user to perform user authentication.”) This authentication process includes the processor(s) *access[ing]* the record in storage to perform the authentication (obtain the biometric template for authentication matching with the user’s input), and

access[ing] the record in storage to release the credential of the record to the requesting resource upon a successful match. *See*, APPL-1006, FIGS. 9, 12, 3:51-4:1, 8:54-9:24 (describing the authentication process). FIG. 9 illustrates authenticating a user after she has enrolled in a website including accessing the record performed by the one or more processors. APPL-1006, 8:54-56.



APPL-1006, FIG. 9, annotated

APPL-1003, ¶¶115-116. With respect to the device of FIG. 2 in the authentication process, the *one or more processors* (executing sensor 204 functions) *access* secure storage 206 to obtain the biometric template of the record so the processor can determine if there is a match of biometric input to said template, and again *access* storage 206 to release the credential and communicate it to the external

resource using application 214 on a successful match. *See* APPL-1006, FIG. 2, 3:44-51, 6:42-49, FIG. 12.

Thus, Kesanupalli discloses this limitation.

[1.3b] wherein the credential information comprises a cryptographic key;

Kesanupalli discloses this limitation. APPL-1003, ¶¶119-121.

As discussed above in [1.3a], Kesanupalli describes a “user credential” (*credential information*), which is a *cryptographic key*. APPL-1006, 3:32- (“password, **cryptographic key**, random seed, and the like.”) *See also*, APPL-1006, 3:65-4:1, 8:6-22, FIG. 12, APPL-1003, ¶¶52-57.

Thus, Kesanupalli discloses this limitation.

[1.4] receive authentication input from the user;

Kesanupalli discloses this limitation. APPL-1003, ¶¶122-124.

As discussed above, Kesanupalli’s functions are performed by one or more processors, which include the functionality of this limitation.

Kesanupalli describes one or more processors *receive an authentication input* (e.g., biometric input such as a fingerprint) *from the user*. Specifically, Kesanupalli describes the processor of sensor (204) receives an authentication input of a fingerprint. APPL-1006, 6:31-34 (“a **fingerprint swipe or fingerprint scan** (using a placement style fingerprint sensor”), 9:10-14 (“FIG. 9 is a flow diagram depicting another embodiment of a procedure 900 for authenticating a

user of a biometric authentication system. Initially, **procedure 900 reads fingerprint information from a user's finger in contact with a fingerprint sensor (902).**”), 8:54-9:3, FIG. 12 user “provide[s] biometrics.”). Kesanupalli also describes other types of authentication input from the user. APPL-1006, 2:30-38.

Thus, Kesanupalli discloses this limitation.

[1.5] determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

Kesanupalli discloses this limitation. APPL-1003, ¶¶125-128.

As discussed above, Kesanupalli's functions are performed by one or more processors, which includes the functionality of this limitation.

Kesanupalli describes its one or more processors (executing functions of sensor 204) *determine[s] the authentication input from the user (fingerprint matches the authentication information associated with the user (fingerprint template) included in the at least one record (bound template and credential) stored on the first device (in secure storage 206).* APPL-1003, ¶126; APPL-1006, 3:32-51 (“During an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor. The process then **determines whether the user's fingerprint information matches a fingerprint template associated with the fingerprint sensor.**”). Kesanupalli describes the processor executing functions of sensor 204 performs the matching:

“For example, in a **successful fingerprint swipe, the swiped fingerprint information matches a fingerprint template** associated with the fingerprint sensor...**biometric sensor 204 includes a ‘match on chip’ functionality that releases a user’s credentials only upon a successful fingerprint swipe or other biometric reading. User credentials and other information may be stored within biometric sensor 204, in a secure storage 206,** or any other storage mechanism.)” APPL-1006, 6:31-49; *see also*, FIGS. 2, 12, 3:52-4:2, 5:9-24, 8:59-9:24.

Thus, Kesanupalli discloses this limitation.

[1.6] retrieve at least a portion of the credential information from the at least one record stored on the first device;

Kesanupalli discloses this limitation. APPL-1003, ¶¶129-132.

As discussed above, one or more processors perform Kesanupalli’s functions, which includes the functionality of this limitation.

As discussed in limitation [1.3a], the *record* (template and credential) is *stored on the first device* (in secure storage 206). Processor circuitry (of sensor 204) *retrieve[s]* the *credential* from the record in storage such that the credential can be transmitted to a requesting resource such as the website. APPL-1006, 9:14-20 (“The procedure then authenticates the fingerprint information (block 904)...If the fingerprint information is authenticated, the **procedure retrieves credentials** associated with the user based on the fingerprint information (block 908).”). In

FIG. 2, processor circuitry (of sensor 204) retrieves the credential from record in storage 206 and provides the credential to PC 202, which in turn sends the credential to the requesting service. *See also*, APPL-1006, FIGS. 2, 8-9, 12, 3:52-4:11, 5:17-32, 6:42-45, 8:59-9:24. Retrieving the credential is retrieving *at least a portion* of the credential information.

Thus, Kesanupalli discloses this limitation.

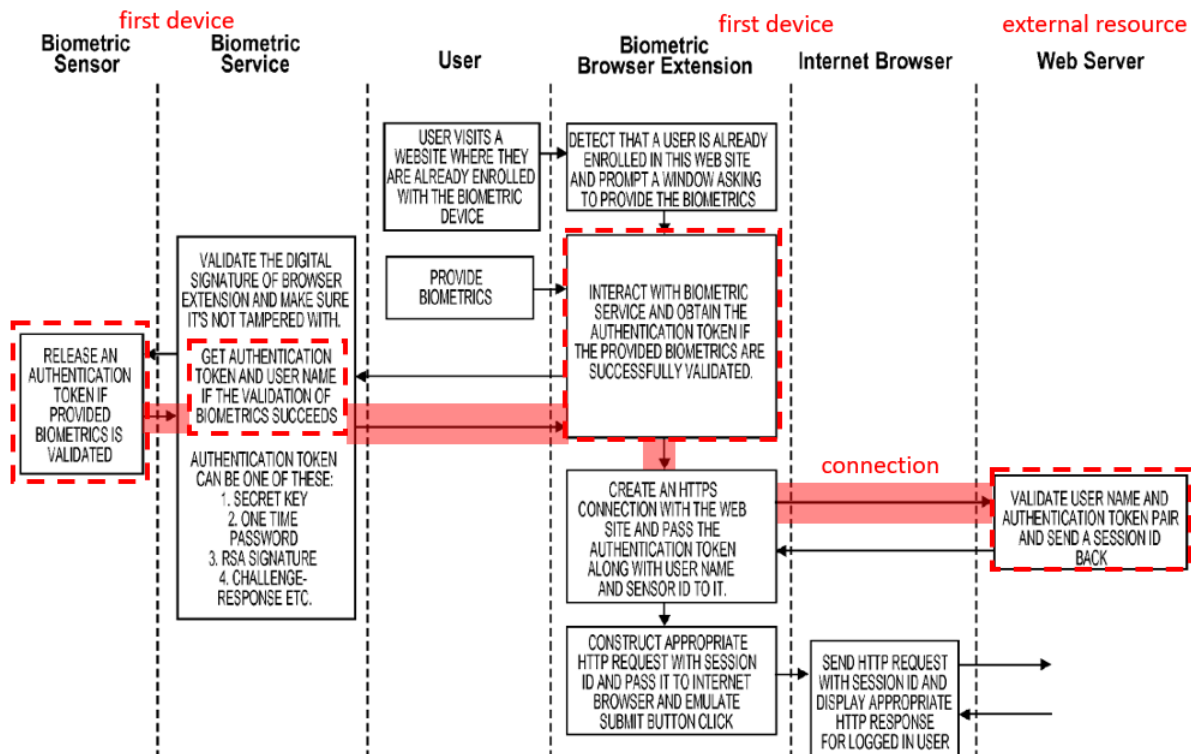
[1.7] facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

Kesanupalli discloses this limitation. APPL-1003, ¶¶133-140.

As discussed above, one or more processors perform Kesanupalli's functions, which includes the functionality of this limitation.

In Kesanupalli's device, one or more processors *facilitate access of the user to the external resource* (website) *at least in part by transmitting, on behalf of the user, from the first device* (storage 206), *output* (user credential) *based at least in part on the at least portion of the credential information retrieved from the at least one record*. *Id.* This is merely executing the translation central to Kesanupalli's disclosure—Kesanupalli describes *transmitting output* (the user credential) from the first device to the *external resource* (website). APPL-1006, 9:4-24 ("If the fingerprint information is authenticated, the procedure **retrieves credentials**

associated with the user based on the fingerprint information (block 908)...The decrypted credentials...are **communicated to a requesting process or system** (block 914).”). In FIG. 2, the user credential (*e.g.*, cryptographic key) is retrieved from secure storage 206 of sensor 204 and provided to application 214 of PC 202 for communication to the external resource. APPL-1006, 6:11-49. FIG. 12 illustrates actions for authenticating a user, including actions performed by a “user,” those actions performed by the user’s device—*e.g.*, by circuitry of the sensor and applications running on Host PC (*e.g.*, biometric service, browser extension, browser applications), and those performed by the external resource’s web server.



APPL-1006, FIG. 12, annotated

APPL-1003, ¶136. *See also*, APPL-1006, 3:52-4:11, 6:42-45, 8:59-9:24 (describing transmitting the credential).

When Kesanupalli transmits the user credential to the requesting website as discussed above, it does so on *behalf of the user* as its the **user's** credential, which is transmitted **in response to the user's request** to access the website. The user credential is *output based at least in part on the at least portion of the credential information* as the output is the user credential itself—*e.g.*, the cryptographic key. *The user of the first device is granted access to the external resource (website) based at least in part on the output (user credential) transmitted from the first device on behalf of the user* because the credential is used to login the user to the external resource. *See* APPL-1006, FIG. 12 (“logged in user”). POSITA would understand when Kesanupalli communicates the credentials “to the Web site to **complete** the user authentication process,” the user is granted access to the website. APPL-1003, ¶138. *See* APPL-1006, 5:22-24. Processing circuitry of sensor 204 facilitates this by transmitting the credential to the processor (PC 202 and application 214), which in turn transmits the credential to the web server of the resource. Sensor 204 and PC 202 provide *one or more processors that facilitate access of the user to the external resource by transmitting the credential information*. APPL-1003, ¶¶135-139.

Thus, Kesanupalli discloses this limitation.

[1.8] *based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record; and*

Kesanupalli, Cheng and Kodama render obvious this limitation. APPL-1003, ¶¶141-150.

As discussed above, one or more processors perform Kesanupalli's functions. Kesanupalli's one or more processors are *operable* and suitable to perform instructions to accomplish the functions of Kesanupalli, and also those backup functions of Cheng and Kodama as discussed below. APPL-1003, ¶142. Cheng and Kodama confirm one or more processors execute their functions. APPL-1008, [0022] (“[o]nboard **microprocessor** and communication means [] handle communication...and other **processing needs** such as establishing a **secure connection** with a remote service bureau, requesting and returning encryption/decryption keys, **creating and copying lower tier and upper tier backup files**, and terminating the connection.”); APPL-1010, [0037] (“Each PC is equipped with...a processing unit (CPU) for processing data stored in the memory”).

First, it would have been obvious for one or more processors to *initiate a backup to [a] second device of a least a portion of the at least one record* of Kesanupalli's device in light of the teachings of Cheng. APPL-1003, ¶¶147-149.

As discussed in the reasons to combine above, Cheng teaches it was a known and desired practice to backup data of a user device such as Kesanupalli's device to provide predictable benefits of maintaining personal data in the event of loss or damage to the device comprising the data.

In particular, Cheng teaches initiating a *backup* of data of a first device to a *second device* in a procedure including registering a first device with a storage location, such as a user service bureau, generating a "backup file(s)" of the device data, and providing the file from the first device to the user service bureau (storage). *See* APPL-1008, Abstract, [0002], [0007]-[0008], [0023]-[0030], FIGS. 3A and 3B. Cheng describes exemplary data for back-up includes user authentication information, such as key and biometric data, which is the same type of data as in Kesanupalli's *record* (user credential and biometric template). APPL-1003, ¶144; APPL-1008 [0007]-[0008], [0030], FIGS. 3A-3B.

Cheng's backup procedure provides the backup data from the storage location (*e.g.*, user service bureau) to a *second device*, which in some implementations is a new device replacing the user's first device. APPL-1008, FIGS. 4A, 5, [0009], [0045]-[0050]. Cheng describes "[t]he **new** biometrics-based authentication **device** establishes a secure connection with a user service bureau, begins the restore process and **downloads backup data from storage.**" APPL-1008, [0048]. *See also*, APPL-1008, FIGS. 4A-4C, [0009], [0031]-[0039]

(restoration). As discussed above, POSITA would recognize applying Cheng's teachings to Kesanupalli's device to backup its *record* would provide a benefit allowing the user to save resources (*e.g.*, time) in recreating the data in the record (*e.g.*, biometric template and/or user credential) on the second device. APPL-1003, ¶146, 87-90. Thus, it would have been obvious to backup to the second device at least a portion of Kesanupalli's record in light of Cheng.

Second, it would have been obvious to *initiate* Cheng's backup to a second device *based at least in part on the first device being a same brand as a second device* as taught by Kodama. APPL-1003, ¶¶147-150. Like Cheng, Kodama discloses a first user device, a backup service (storage), a second user device, and a procedure of backing up data of the first user device to the storage service for downloading by a second device. APPL-1010, [0034], [0040]-[0041], [0101], [0106], FIG. 13. Also like Cheng, Kodama's procedure begins with registering a first device with a backup service and includes the registration provides "[first] device information including the **manufacturer name**." APPL-1010, [0101]. POSITA would understand the "manufacturer name" to constitute a *brand* of the device in Kodama. APPL-1003, ¶148. Kodama's backup service "adds the received information to the backup device registration table." APPL-1010, [0103]. *See also*, APPL-1010, [0078]-[0104] (service registration), FIG. 4 ("manufacturer name 0403"), [0054], FIG. 6, [0061] ("example of the device information. This

table is configured from a manufacturer name 0601...and is used upon registering the backup device in the online backup service system.”) Kodama continues the backup process by sending a copy of the data of the registered first device to the backup service. APPL-1010, [0106]–[0107]. *See also*, APPL-1010 [0108]–[0118].

Kodama continues its backup procedure by providing a *second device* associated with the user, which is registered with the backup service. In an example, the second device is a user’s “new” device. APPL-1010, [0160]. In Cheng, downloading or restoring the stored backup data onto the second device includes “verifying registration information of the user with a user service bureau.” APPL-1008, [0032]. *See also*, APPL-1008, FIG. 4A, [0047]. Kodama again expands on this registration illustrating it includes providing “[second] device information including the **manufacturer name**” to the backup service. APPL-1010, [0135]–[0136]. The backup service then “**checks** whether there is an entry where the user account name, device name and **device information coincides**.” APPL-1010, [0137]. Kodama describes “[t]he **restoration is permitted when the manufacturer name and the model number of the restoration target appliance coincide**. This embodiment explains a case where restoration is **permitted only** with the same model of the **same** manufacturer.” APPL-1010 [0138]. Restoration only to the same manufacturer/model means *initiating* backup

to the second device is based at least in part on the manufacturer being the same. APPL-1003, ¶148. Therefore, Kodama discloses or suggests *initiating a backup* to a second device based *at least in part on* the brand (*e.g.*, manufacturer name) of the first device being the same as the second device.

Thus, Kesanupalli, Cheng and Kodama renders obvious this limitation.

[1.9] *a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.*

Kesanupalli discloses this limitation. APPL-1003, ¶¶151-154.

Kesanupalli's system includes a main memory, *a memory*. APPL-1006, 10:26-47 (“**Main memory** is also usually included for storing and retrieving larger amounts of information such as data and software applications configured to **perform functions** according to the invention when executed by the central processing unit.”) POSITA would understand that the main memory of Kesanupalli's system would be coupled to the *one or more processors* and configured to provide the one or more processors with *instructions*. APPL-1003, ¶153. For example, Kesanupalli explains application 112 of PC 202 “executes on a host PC 102.” APPL-1006, 5:59-66. An application executing on a PC requires instructions for its execution to be stored in a memory. APPL-1003, ¶153.

Thus, Kesanupalli teaches this limitation.

Therefore, claim 1 is obvious over Kesanupalli, Cheng and Kodama. APPL-1003, ¶155.

6. Claim 14

[14.0] *The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.*

Kesanupalli, Cheng and Kodama render obvious all the limitations of claim 1 and Kesanupalli discloses this further limitation. APPL-1003, ¶¶156-158.

As illustrated above, Kesanupalli's authentication input is a biometric input of the user, which is *received using a biometric user input element* such as a fingerprint sensor. APPL-1003, ¶157; APPL-1006, 2:39-53 ("Certain described embodiments refer to 'swipe' style **fingerprint sensors**. However, alternate embodiments may include **any type of fingerprint sensor**, such as a 'placement' sensor.")

Therefore, claim 14 is obvious over Kesanupalli, Cheng and Kodama.

7. Claims 18 and 33

Claims 18 and 33 are obvious over Kesanupalli, Cheng and Kodama. APPL-1003, ¶¶159-162. The limitations of independent claim 18, except the preamble of the claim, are substantively identical to limitations of claim 1 addressed above, as correlated in the table below:

Claim 18 Limitation	Corresponding Limitation of Claim 1 illustrating the limitation of Claim 18 is disclosed in Kesanupalli, Cheng, and/or Kodama

[18.1] <i>receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;</i>	[1.2]
[18.2] <i>accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential information comprises a cryptographic key;</i>	[1.3a], [1.3b]
[18.3] <i>receiving authentication input from the user;</i>	[1.4]
[18.4] <i>determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;</i>	[1.5]
[18.5] <i>retrieving at least a portion of the credential information from the at least one record stored on the first device;</i>	[1.6]
[18.6] <i>facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and</i>	[1.7]
[18.7] <i>based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.</i>	[1.8]

[18.0] *A method, comprising:*

To the extent the preamble is limiting, Kesanupalli, Cheng and Kodama

disclose it. The citations in the analysis above apply to a *system* in claim 1 and also to a *method*. APPL-1003, ¶160; APPL-1006, 2:30-38 (“The systems and **methods** described herein relate to biometric authentication of users...”), 10:48-54, FIGS. 7, 9.

Thus, claim 18 is obvious over Kesanupalli, Cheng and Kodama.

Dependent claim 33 is substantively identical to claim 14, except that it depends from method claim 18. Kesanupalli, Cheng and Kodama render obvious claim 33 for the same reasons as claims 14 and 18. APPL-1003, ¶162.

8. *Claim 35*

Claim 35 is obvious over Kesanupalli, Cheng and Kodama. APPL-1003, ¶¶163-166. The limitations of claim 35, except the preamble, are substantively identical to limitations of claim 1, as correlated in the table below:

Claim 35 Limitation	Corresponding Limitation of Claim 1 illustrating the limitation of Claim 18 is disclosed in Kesanupalli, Cheng, and/or Kodama
[35.1] <i>receiving, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;</i>	[1.2]
[35.2] <i>accessing at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access, wherein the credential</i>	[1.3a], [1.3b]

<i>information comprises a cryptographic key;</i>	
<i>[35.3] receiving authentication input from the user;</i>	[1.4]
<i>[35.4] determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;</i>	[1.5]
<i>[35.5] retrieving at least a portion of the credential information from the at least one record stored on the first device;</i>	[1.6]
<i>[35.6] facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and</i>	[1.7]
<i>[35.7] based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.</i>	[1.8]

[35.0] A computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for:

To the extent the preamble is limiting, Kesanupalli discloses it. The citations to Kesanupalli, Cheng and Kodama above apply to a *system* as in claim 1, and also to the recited *computer program*. APPL-1003, ¶165. Kesanupalli discloses a *computer program product* comprises instructions for the processor(s) including those instructions executed by its sensor 204 and a computing host (PC)

202 discussed above. *See* APPL-1006, 9:58-10:12 (“configured to perform particular tasks according to the invention, by executing machine-readable software code that defines the particular tasks embodied by the invention.”), 13:8-39.

Thus, claim 35 is obvious over Kesanupalli, Cheng and Kodama.

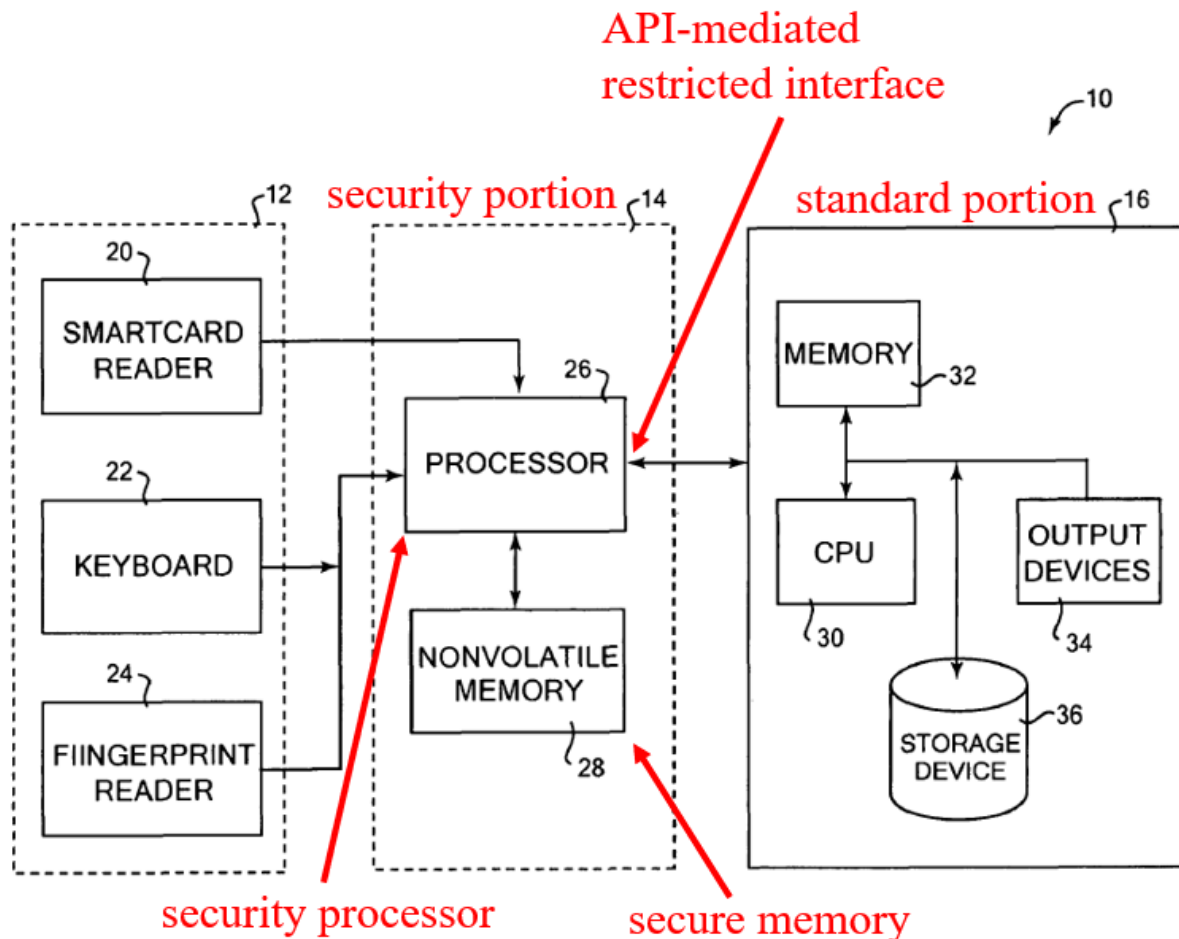
B. Ground 2: Claims 9-11 and 28-30 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng, Kodama and in further view of Challenger.

1. Challenger

Challenger “relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features.” APPL-1007, 1:7-9, 3:24-26. *See also*, APPL-1003, ¶¶167-169. Challenger illustrates a system 10 (*e.g.*, computer or electronic device) with a system architecture suitable for securing data and functions of system 10 from unauthorized access and manipulation. APPL-1007, 3:37-56. Challenger describes system implementations in accord with a well-known Trusted Platform Module (TPM) specification promulgated by the Trusted Computing Group (TCG). *See* APPL-1007, 3:51-56. As explained in Challenger, under the TPM specification, a standard chipset including a programmable microcontroller can be provided and used to store and secure information of the system that is desired to be protected. APPL-1003, ¶167.

Broadly speaking, TPMs provide a platform for effective trusted computing

features. APPL-1003, ¶¶168, 58-61. The security architecture (*i.e.*, the processor “functions and the application program interface (API)” that runs on the processor) can be referred to as a TPM. A TPM also offers a variety of features, including a random number generator, facilities for secure generation of cryptographic keys, and abilities to limit the use of keys, *e.g.*, to signing and verification, and/or encryption and decryption. APPL-1007, 1:18-31 APPL-1003, ¶168; APPL-1017 (TPM standard describing API mediated restricted interface).



APPL-1007, FIG. 1, annotated

Challenger provides an implementation framework for secure systems, which is TPM-based, and which includes an input portion 12, a security portion 14, and a standard portion 16. *See* APPL-1007, 3:46-57. Security portion 14 includes a dedicated security processor 26 (implementing a TPM architecture) and memory 28 used to secure data and applications of the system for access and use only by authorized users. APPL-1007, 4:9-65. Memory 28 is connected to processor 26 and “is a secure memory which cannot be easily tampered with to read its data contents” and can be on the same chip or package as the memory 28. *Id.* Standard portion 16 is connected to security processor 26 (via its API-mediated interfaces) and includes microprocessor 30 that controls general operation of the system including input/output functions. APPL-1007, 5:15-25.

2. Reasons to Combine Kesanupalli, Cheng, Kodama and Challenger

POSITA would have been motivated to apply Challenger’s teachings of a TPM-type security architecture (with its API-mediated interfaces between secure portions and less-secure portions) in implementations of Kesanupalli’s secure user authentication techniques using biometric information with Cheng/Kodama’s backing up of personal data teachings. APPL-1003, ¶¶170-174. The combination would have produced the obvious, beneficial, and predictable results of a standardized, widely-deployed, security architecture for implementation of

Kesanupalli and Cheng/Kodama's techniques as discussed below. *Id.*

First, Challenger, Kesanupalli, Cheng, Kodama and the '105 patent are analogous art and are all in the same field of endeavor—namely, information security, and more particularly, security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. APPL-1003, ¶171; APPL-1007, 1:7-9 (“The present invention relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features.”), 3:52-56 (“Trusted Platform Module (TPM)...for securing data and functions of the system [] from unauthorized access and manipulation.”); *see* Section IX.A.4 (reasons to combine Kesanupalli, Cheng, Kodama). Moreover, Challenger bears the very IPC subclass—G0F6 21 as discussed above. APPL-1007, (51); *see supra* IX.A.4.

Second, POSITA would have been motivated to apply Challenger's teachings of a standards-based TPM architecture as an implementation framework for Kesanupalli's biometric security techniques given the support that a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided. APPL-1003, ¶172; APPL-1007, 1:18-31 (summarizing typical TPM functions and APIs). Indeed, Challenger's description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data, *e.g.*, “secure hash

values and...keys,” *and* fingerprint reader 24 behind a security processor 26 that “implements the particular security features and functions (*e.g.*, API functions, algorithms)” in a system that includes secure and non-secure portions. APPL-1007, 4:57-5:9, 3:67-4:23. As Kesanupalli relies on these features to perform its authentication (*e.g.*, sensor 204), they are precisely the security architecture features POSITA having Kesanupalli before them would be motivated to implement in a standards-based security architecture to engender trust amongst users and customers. APPL-1003, ¶58-61, 172.

Finally, POSITA would have had reasonable expectations of success in implementing Kesanupalli’s biometric authentication techniques with Cheng/Kodama’s backup features with Challenger’s architecture as Challenger’s architecture applies TPM techniques, which were well-known, standard and widely-deployed in the industry. APPL-1003, ¶¶174, 58-61; APPL-1024 illustrating widespread adoption. *See* APPL-1007, 1:18-31; *see also* Section IX.B.1.

3. Claim 9

[9.0] *The system of claim 1,*

[9.0a] *wherein the at least one record stored on the first device is stored in a secure storage, and*

[9.0b] *wherein the one or more processors are configured to access the at least one record stored on the secure storage using a restricted interface.*

Claim 9 is obvious in light of Kesanupalli, Cheng, Kodama and Challener. APPL-1003, ¶¶175-183. As shown in limitation [1.3a] above, Kesanupalli discloses *at least one record stored on the first device*, and in particular, discloses that the *record* is stored in “secure storage 206,” which is a *secure storage*, as claimed. See APPL-1006, FIG. 2, 6:45-49. POSITA would understand *secure storage* is protected from unauthorized use and by describing storage as “secure storage,” Kesanupalli indicates its storage is protected from unauthorized use. APPL-1003, ¶176. FIG. 2 confirms this as use and access to secure storage 206 is controlled by sensor 204, and the storage is not directly accessible by others (e.g., application 214 executing on Host PC 202); for example, the user credential in the storage cannot be accessed except by sensor 204 when verifying a match of biometric input as discussed in limitation [1.5]. Therefore, secure storage 206 is *secure storage*, which discloses [9.0a] and this secure storage maintains its protected character when implemented in Challener’s secure architecture. APPL-1003, ¶¶175-176; APPL-1007, FIG. 1, 4:56-65 describing memory 28 in security portion 14 connected to the processor 26, “memory 28 is a secure memory which

cannot be easily tampered with to read its data contents. [and] can be included on the same integrated circuit chip, or package, or the processor 26.”

Continuing to [9.0b], as discussed above at limitation [1.3a], Kesanupalli teaches *the one or more processors are configured to access the at least one record stored on the device, and providing this access using a restricted interface* is obvious in view of Challener. APPL-1003, ¶¶177-183.

As described above, it would have been obvious to implement functionality of Kesanupalli’s system (particularly, processing circuitry of sensor 204 and its interface with secure storage 206) within the secure portion of the TPM security architecture taught by Challener. APPL-1003, ¶¶170-174; APPL-1007, 4:9-24 (“The **processor 26 typically implements a ‘security architecture’** which, as used herein, refers to the particular security features and functions (*e.g.* **API functions**, algorithms) implemented for the system 10 as determined by a security architecture application loaded on the processor 26.”), FIG. 1. As indicated above, the security architecture of Challener implements a nonvolatile memory 28 integrated with and physically connected to secure processor 26 to hold secure data. Nonvolatile memory 28 stores secure data pertinent to performing the security functions of the processor—just like secure storage 206 of Kesanupalli. APPL-1007, 5:5-7.

In Kesanupalli implemented on Challener’s architecture, the security

processor (sensor 204) is configured to access the record stored in secure storage using a *restricted interface*, as that term is explained in the '105 patent. Kesanupalli suggests that its secure storage 206 is “within the biometric sensor 204.” APPL-1006, 6:45-47. Challenger further describes secure storage is not merely in a same device, but “included on the same integrated circuit chip.” APPL-1007, 4:63-65. This is precisely one of the example *restricted interface[s]* of the '105 patent. APPL-1001, 18:53-55. POSITA would also recognize Challenger teaches the memory may be integrated with the processor, which is yet another example of a *restricted interface* in the '105 patent. APPL-1007, 9:49-51; APPL-1003, ¶179.

As explained above, “*restricted interface*” is an interface that limits accessibility. Furthermore, based on the '105 patent’s description, POSITA would understand “*restricted interface*” to at least include an API that limits accessibility. See Section VI.A.; APPL-1003, ¶180-183. In particular, Kesanupalli (implemented using Challenger’s TPM framework for secure systems) provides communication between the security portion (14), including processor (26) and its secure storage (28), and the standard portion (16) occurs through a *restricted interface* as detailed below.

TPM-based implementations, including Challenger’s TPM-based implementation, are widely recognized examples of a security architecture

providing a *restricted interface* in the form of an access limiting API to restrict access to the TPM (secure processor) by programs running on a general processor in a standard (non-secure) portion of a system to the security-related operations and data, such as key and credential management, secure storage, encryption, decryption and digital signatures, that are provided in a secure portion of the system. *Id.* See also, APPL-1007, 4:3-15 discussing controlling “access.” The Board has itself recognized, in the context of the related ’696 patent, that TPM implementations disclose a “*restricted interface*.” See (Samsung ’696 Patent IPR) IPR2022-00244, Paper 17, 40.

Challenger discloses an interface (an API) used in the communication of the general processor and the secure storage in its TPM-based architecture. This is because access to the memory must be via the secure processor (26) of Challenger, which implements a security architecture that includes API functions used in its communication with other components—including the general processor 30. APPL-1007, 4:9-24 (“The **processor 26 typically implements a ‘security architecture’** which, as used herein, refers to the particular security features and functions (*e.g.* **API functions**, algorithms) implemented for the system 10 as determined by a security architecture application loaded on the processor 26.”), FIG. 1. An API is an interface that defines how two components—here the software on processor 26 and the software on general processor 30—communicate

with one another. APPL-1003, ¶¶182, 61. And a TPM-based API, such as provided by Challenger's processor 26, provides restrictions by the way of a set of rules or restrictions POSITA would understand are defined by the TPM standard for access to the security portion 16 of the system. *Id.*

Thus, implementing Kesanupalli (as modified by Cheng/Kodama) using the architecture of Challenger provides communication between the general processor (PC 202) and security processor (sensor 204) via a *restricted interface* (e.g., via an API of the TPM security architecture of the security processor executing the processor functions of sensor 204). This is merely a predictable use of a known element according to its established function in the TPM architecture.

Thus, claim 9 is also obvious over Kesanupalli, Cheng, Kodama and Challenger.

4. Claim 10

[10.0] The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

As discussed above with respect to claim 9, Kesanupalli implemented on Challenger's TPM includes a *dedicated physical connection* between the secure processor circuitry and the secure memory rendering obvious claim 10. APPL-1003, ¶184. The secure memory is accessible **only** via the secure processor and thus, has a dedicated connection to the memory. *See also*, APPL-1006, FIG. 2; APPL-1007, FIG. 1. The memory is physically "on-chip" or integrated with the

processor, thus is a dedicated physical connection such as a dedicated chip level conductive interconnect between the secure processor circuitry and its associated memory. APPL-1007, 4:60-65, 9:49-51; APPL-1003, ¶¶184, 167-169, 177-183, 63, 58-61. Therefore, POSITA would recognize a restricted interface of a dedicated physical connection would have been obvious in light of Challener's teachings. Thus, claim 10 is obvious over Kesanupalli, Cheng, Kodama, and Challener. APPL-1003, ¶184.

5. Claim 11

[11.0] The system of claim 9, wherein the restricted interface comprises an application programming interface.

As discussed above with respect to claim 9, Challener's TPM-based implementation is an example of a security architecture that provides a *restricted interface* in the form of an access limiting API. APPL-1003, ¶180-183; APPL-1007, 4:3-15. In the applied combination, Kesanupalli is implemented on Challener's TPM architecture, and the TPM-based API is part of a *restricted interface* that limits access to secure storage/memory by one or more processors (e.g., at least limiting access of Kesanupalli's Host PC functionality implemented in the standard portion of Challener's TPM architecture). APPL-1003, ¶¶167-169, 177-183, 58-61. Thus, claim 11 is obvious over Kesanupalli, Cheng, Kodama, and Challener. APPL-1003, ¶¶185-186.

6. Claims 28-30

Dependent claims 28-30 are substantively identical limitations to claims 9-11 addressed above but depend from method claim 18. Kesanupalli, Cheng, Kodama and Challenger render obvious these claims for the same reasons as discussed above with respect to claims 9-11 and 18. APPL-1003, ¶¶187.

C. Ground 3: Claims 1, 9-11, 14, 18, 28-30, 33 and 35 are obvious under 35 U.S.C. §103 over Jakobsson '351 and Kodama.

1. Jakobsson '351 and Kodama

Jakobsson '351 is an issued patent stemming from U.S. Application No. 15/042,636, which is an application to which the '105 patent claims priority (through a CIP). As noted above, Jakobsson '351 does not contain written description of the Challenged Claims of the '105 patent as it lacks a teaching of “based at least in part on the first device being a same brand as a second device, initiat[e/ing] a backup, to the second device,” a limitation of each of the Challenged Claims. APPL-1003, ¶¶36-41, 188. Kodama discloses this limitation and would be obvious to combine with Jakobsson '351; Kodama is discussed above at Section IX.A.3. Tellingly the Examiner set forth a double patenting rejection of the claims during the prosecution leading to the '105 patent over Jakobsson '351.

2. Reasons to Combine Jakobsson '351 and Kodama

It would be obvious to combine Jakobsson '351 and Kodama as POSITA

would have been motivated to apply Kodama's teachings of ensuring devices in the backup technique such as in Jakobsson '351 are of the same brand, which provides the obvious, beneficial and predictable result of mitigating compatibility and security issues that may arise between brand differences when transferring data. APPL-1003, ¶¶189-192.

First, Jakobsson '351, Kodama and the '105 patent are in the same field of endeavor as each is directed to an environment of a plurality of devices such as client devices and backup systems interacting over a network. APPL-1003, ¶189; APPL-1011, FIG. 1; APPL-1010, FIG. 1; APPL-1001, FIG. 1. And each is also concerned with transfer, protection, and back up of data associated with the devices of the environment. APPL-1010, [0040], [0041], [0159]; APPL-1011, 12:13-20; APPL-1001, 1:43-50. As Jakobsson '351 is within the priority chain of the '105 patent it is evident they are in the same field of endeavor; and Kodama is similarly directed to client devices and backup systems interacting over a network, the security of data when transferring such data. APPL-1010, FIG. 1, [0006]-[0007] including "mitigating the risk of a third party referring to or using backup data without authorization upon restoring such backup data." *See also* APPL-1001, (51), (52); APPL-1011, (52), APPL-1010, (51).

Second, POSITA would have found it predictable to apply Kodama's teachings to Jakobsson '351's backup process. APPL-1003, ¶190. Jakobsson '351

describes the desire to back up or synchronize data across a user's devices. APPL-1011, 7:37-41. However, Jakobsson '351 neglects to consider properties of synchronized devices that may affect this synchronization; Kodama recognizes "if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of data between the products will differ." APPL-1010, [0157]. POSITA would recognize this differing format can create compatibility issues and thus would recognize an advantage of, and reason for, basing the initiation of data transfer to the second device on brand and thereby avoiding these compatibility issues as taught by Kodama. APPL-1003, ¶190. Kodama also describes its methods and system provide a benefit of being "capable of mitigating the risk of a third party referring to or using backup data without authorization upon restoring such backup data in an electronic appliance." APPL-1010, [0007]. One way it provides this benefit is by ensuring the source and target devices are the same brand and therefore have similar safeguards.

POSITA would have also had a reasonable expectation of success in applying Kodama's teachings. APPL-1003, ¶192. Kodama states: "Conventionally, technology of backing up data in a PC to an external recording medium...and restoring the backed up data in the PC is **widely known**." APPL-1010, [0003]. Initiating a backup technique based on a brand is a simple addition

of routine software executed on generic processing components. APPL-1003, ¶192.

3. Claim 1

[1.0] A system, comprising:

Jakobsson '351 provides *a system*, which is summarized in its claim 1. APPL-1003, ¶¶193-194; APPL-1011, 10:50 (“1. A system, comprising:”). As described below, Jakobsson '351 claim 1 provides, except for the backup initiating, substantially similar limitations as those of claim 1 of the '105 patent.

Jakobsson '351 discloses this limitation.

[1.1] one or more processors configured to:

Jakobsson '351 at claim 1 recites its system comprises “one or more processors configured to” perform its functions as discussed in the following elements. APPL-1011, 10:51.

Jakobsson '351 discloses this limitation. APPL-1003, ¶¶195-196.

[1.2] receive, at a first device, a request to access a resource external to the first device, wherein the resource external to the first device is associated with a user;

Jakobsson '351 claim 1 discloses a system with one or more processors configured to “...**receive**, at an authentication translator **at a device**, an authentication input and an indication of a **request**, by a user of the device, to **access a resource external to the device**” APPL-1011, 10:52-55. The resource is

associated with the user as it is requested by the user.

Jakobsson '351 discloses this limitation. APPL-1003, ¶¶197-198.

[1.3a] access at least one record stored on the first device, the at least one record including authentication information associated with the user and credential information associated with the external resource to which the user has requested access,

[1.3b] wherein the credential information comprises a cryptographic key;

Jakobsson '351 claim 1 also discloses these limitations:

...in response to determining, by the authentication translator at the device, a match using the received authentication input, **obtain access to a record stored on the device, wherein the record is associated at least with the external resource;**

retrieve, **from the stored record** accessed at least in part by determining, by the authentication translator at the device, the match using the received authentication input, **a previously stored credential associated with the external resource**, wherein the previously stored credential is different from the received authentication input, and wherein the previously stored credential retrieved from the record stored on the device comprises at least one of a **cryptographic key** and a cookie[.]

APPL-1011, 10:56-11:3. Jakobsson '351 system also uses a “template” stored in the record for its match; the template comprises “at least one of a fingerprint feature, a voice biometric feature, a facial recognition feature, an iris detection feature, and a retina scan feature,” which are *authentication information associated with a user*. APPL-1011, 11:22-24, 12:8-12. *See also*, APPL-1011, 11:45-56,

FIG. 2.

Jakobsson '351 discloses this limitation. APPL-1003, ¶¶199-202.

[1.4] receive authentication input from the user;

[1.5] determine that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;

Jakobsson '351 at claim 1 also discloses that one or more processors of its system: “**receive**, at an authentication translator at a device, **an authentication input** and an indication of a request, **by a user** of the device, to access a resource external to the device.” APPL-1011, 10:51-55.

Jakobsson '351 continues to recite its one or more processors of the system “in response to **determining, by the authentication translator at the device, a match using the received authentication input**, obtain access to a record stored on the device, wherein the record is associated at least with the external resource.” APPL-1011, 10:56-60. As discussed in limitation [1.3a], a template is *authentication information associated with the user included in the at least one record stored on the first device* and is used for the matching. See also, APPL-1011, 11:45-50, FIG. 2, 4:55-68.

Jakobsson '351 discloses these limitations. APPL-1003, ¶¶203-206.

[1.6] retrieve at least a portion of the credential information from the at least one record stored on the first device;

Jakobsson '351 further discloses in its claim 1 that one or more processors

of its system “**retrieve, from the stored record** accessed at least in part by determining, by the authentication translator at the device, the match using the received authentication input, **a previously stored credential** associated with the external resource...” APPL-1011, 10:61-11:30. *See also*, APPL-1011, 12:4-7.

Jakobsson ’351 discloses this limitation. APPL-1003, ¶¶207-208.

[1.7] facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and

Jakobsson ’351 further discloses in its claim 1 that one or more processors of its system “establish a connection between the device and the external resource to which the user requested access; and **facilitate a login of the user to the external resource at least in part by transmitting, on behalf of the user, from the device and via the established connection, output based at least in part on the at least one of the cryptographic key and the cookie retrieved from the record** accessed at least in part by determining, by the authentication translator at the device, the matching using the received authentication input, **wherein the user of the device is logged into the external resource based at least in part on the output transmitted from the device on behalf of the user.**” APPL-1011, 11:4-18.

Jakobsson ’351 discloses this limitation. APPL-1003, ¶¶209-210.

[1.8] *based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device, of at least a portion of the at least one record; and*

Jakobsson '351 in view of Kodama renders obvious this limitation. APPL-1003, ¶¶211-217.

First, Jakobsson '351 discloses that its system and processors are further configured to: encrypt and authenticate at least a portion of the record; and **perform a backup** of the encrypted and authenticated **record** to a remote storage entity, wherein the remote storage entity is configured to synchronize records **between at least two devices** associated with the user.” APPL-1011, 12:13-20.

It would have been obvious to initiate Jakobsson '351's backup of a record to the second device *based at least in part on the first device being a same brand as a second device*. Like Jakobsson '351, Kodama also teaches a first user device, a backup service, and a second user device, and a procedure of backing up data of the first user device to a second device can involve the backup service (“remote storage entity” in Jakobsson '351).

As discussed above in Sections IX.A.3, Kodama teaches registering a first device with a backup service explains that this registration includes “device information including the manufacturer name, model name.” APPL-1010, [0101]. POSITA would understand at least “manufacturer name” to constitute a *brand* of a device. APPL-1003, ¶216. Kodama's backup service “adds the received

information to the backup device registration table.” APPL-1010, [0103]. *See also*, APPL-1010 [0078]–[0104], FIG. 4, [0054], FIG. 6, [0061]. Kodama then continues the backup process by sending a copy of registered first device’s data to the backup service. APPL-1010 [0106]–[0107]. *See also*, APPL-1010 [0108]–[0118]. Thus, Kodama teaches providing a brand of the first device to the backup service.

Kodama further provides a *second device* associated with the user that is registered with the backup service. In an example, the second device is a “new” device of the user. APPL-1010, [0160], [0157], [0137]. Kodama describes registering the second device with the backup service by providing “device information including the manufacturer name, model name and product serial number.” APPL-1010, [0135]–[0136]. The backup service system then “checks whether there is an entry where the user account name, device name and device information **coincides**.” APPL-1010 [0137]. “[T]he restoration is permitted when the manufacturer name and the model number of the restoration target appliance coincide. This embodiment explains a case where **restoration is permitted only with the same model of the same manufacturer**.” APPL-1010 [0138]. Permitting restoration only when the manufacturer and model are the same means that *initiating* of backup to the second device is based on the manufacturer being the same—i.e., brand is the same. *See also*, APPL-1010 [0143]–[0144]. Therefore,

Kodama discloses *initiating a backup* to a second device based *at least in part on* the brand (*e.g.*, manufacturer name) of the first device being the same as the second device. POSITA would have had reason, and found obvious, to apply Kodama's teaching to the system of Jakobsson '351 for at least the compatibility reasons described in Kodama.

Thus, Jakobsson '351 and Kodama render obvious this limitation.

[1.9] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

Jakobsson '351 further recites in its claim 1 that its system includes “a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.” APPL-1011, 11:19-21.

Thus, Jakobsson '351 discloses this limitation. APPL-1003, ¶¶218-219.

Therefore, claim 1 is obvious over Jakobsson '351 and Kodama. APPL-1003, ¶220.

4. Claims 9-11

[9.0] The system of claim 1, wherein the at least one record stored on the first device is stored in a secure storage, and wherein the one or more processors are configured to access the at least one record stored on the secure storage using a restricted interface.

[10.0] The system of claim 9, wherein the restricted interface comprises a dedicated physical connection.

[11.0] The system of claim 9, wherein the restricted interface comprises an application programming interface.

Jakobsson '351 further describes its system includes “a secure

storage...wherein the record is stored in the insecure storage, and wherein obtaining access to the record comprises loading the record to the secure storage.” APPL-1011, 11:57-56.

Jakobsson '351 also describes its processors are configured to access the at least one record stored on the secure storage using a restricted interface. APPL-1011, 3:54-63 including “processor can only communicate with the dedicated processor/sensor via a **restricted API**.” Thus, claims 9 and 11 are obvious over Jakobsson '351 and Kodama. APPL-1003, ¶¶221-222, 224-225.

FIG. 3 of Jakobsson illustrates “secure storage 306 attached to a dedicated processor 308.” APPL-1011, 4:7-8. POSITA would have found it obvious to interface the secure storage with its dedicated processor using a *dedicated physical connection*. Because a dedicated processor is the only disclosed access to the secure storage, a dedicated physical connection would be an obvious implementation choice. APPL-1003, ¶223; APPL-1011, 3:54-63 (“processor can only communicate with the dedicated processor/sensor via a restricted API”). Thus, claims 9 and 10 are obvious over Jakobsson '351 and Kodama. APPL-1003, ¶¶221-223.

5. Claim 14

[14.0] *The system of claim 1, wherein the authentication input from the user is received using a biometric user input element.*

Jakobsson '351 explains its system includes “a biometric input component,”

that provide “a biometric input.” APPL-1011, 11:22-26, 45-50.

Therefore, claim 14 is obvious in light of Jakobsson ’351 and Kodama. *See* APPL-1003, ¶¶226-227.

6. Claims 18, 28-30 and 33

The limitations of independent claim 18, except its *method* preamble, are substantively identical to limitations of claims already addressed above. Jakobsson ’351 similarly includes method claim 17, which is substantially similar to the cited system of claim 1 of Jakobsson ’351 discussed above. The chart below illustrates the citations of Jakobsson ’351, which apply to claim 18 in conjunction with the citations and analysis discussed with respect to Jakobsson ’351’s claim 1 above, which equally apply here. APPL-1003, ¶¶228-230. Thus, claim 18 is obvious in light of Jakobsson ’351 and Kodama.

Claim 18 Limitation (see Ground 1 chart)	Additional Disclosure Jakobsson ’351	Applicable Analysis above
[18.0] <i>A method, comprising:</i>	12:21	
[18.1] <i>receiving...;</i>	12:22–25	[1.2]
[18.2] <i>accessing at least one record...;</i>	12:26-39, 56-58	[1.3]
[18.3] <i>receiving authentication input from the user;</i>	12:22–25	[1.4]
[18.4] <i>determining that the authentication input from the user matches...;</i>	12:26-30	[1.5]

[18.5] <i>retrieving...;</i>	12:31-39	[1.6]
[18.6] <i>facilitating...; and</i>	12:40-53	[1.7]
[18.7a] <i>based at least in part on the first device being a same brand as a second device,</i> [18.7b] <i>initiating a backup, to the second device, of at least a portion of the at least one record.</i>	As to [18.7b], 14:16-22	[1.8]

Dependent claims 28-30 and 33 are substantively identical to claims already addressed above, as correlated in the table below. Jakobsson '351 and Kodama render obvious these claims for the same reasons discussed above with respect to claim 18 and the corresponding claims in of the table. APPL-1003, ¶230.

Claim	Additional Jakobsson '351 disclosure	Corresponding Claim Analysis above
[28]	13:17-23	[9]
[29]		[10]
[30]		[11]
[33]	12:65-13:2	[14]

7. Claim 35

The preamble of claim 35 is directed to a computer program product...comprising computer instructions for.” To the extent it is limiting, Jakobsson '351 discloses this. See APPL-1011, 1:57-2:7. The remaining limitations of claim 35 are substantively identical to limitations of claim 1 already addressed above and thus, claim 35 is obvious for the same reasons. The correlation table provided at Section IX.A.8 is equally applicable. Thus, claim 35

is obvious over Jakobsson '351 and Kodama. APPL-1003, ¶¶231-233.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

The Board should not exercise its discretion under 35 U.S.C. §§314(a) or 325(d) to deny this Petition.

A. The *Fintiv*⁵ factors favor institution.

Denial would be improper based on factors in *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). Patent Owner asserted the '105 patent against Apple in WDTX-1-23-cv-00324 (“the Parallel District Court Proceeding”). *See* Section II.B

First, this Petition presents compelling evidence of unpatentability of the Challenged Claims. *See* Section IX. Therefore, the Board should not deny institution based on parallel litigation. APPL-1025, 2, 4-5, 9 (Director Memo).

Second, the *Fintiv* factors weigh in favor of institution.

- Factor 1 is neutral. Apple has not yet requested a stay pending resolution of this IPR.

⁵ Apart from Apple’s showing *Fintiv* favors institution, the *Fintiv* framework should not be followed because it is legally invalid. The framework (1) exceeds the Director’s authority, (2) is arbitrary and capricious, and (3) was adopted without notice-and-comment rulemaking.

- Factors 2 and 5 favor institution. Although the current scheduling order projects a trial date of December 4, 2024 (APPL-1028, 4), median time-to-trial statistics for WDTX indicate 25.8 months (mid-June 2025, based on March 24, 2023 complaint). *See* APPL-1027, 8-9 (median time-to-trial, generally), 37 (WDTX statistics). Here, final written decision is due July 2025. Per the Director’s Memo, PTAB will weigh factor 2 against exercise of discretion “if the median time-to-trial is around the same time or after the projected statutory deadline for the PTAB’s final written decision.” APPL-1025, 9. Inefficiency concerns are minimal.
- Factors 3 and 4 favor institution: The Parallel District Court Proceeding is in its early stages. Preliminary contentions have been served, a Markman hearing was held December 12, 2023, and fact discovery just opened. At the hearing, the Court indicated it was adopting preliminary constructions and denied Apple’s motion for transfer to NDCA, though no written order has issued. Preliminary constructions apply plain and ordinary meaning. APPL-1026, 1-2. This Petition is not duplicative because it challenges claims 10 and 29 which are not asserted in the Parallel District Court Proceeding. *See* APPL-1029, 2. Moreover, Apple stipulates that, if the Board

institutes this Petition and IPR2024-00507, it will not pursue the grounds raised in either petition in the Parallel District Court Litigation with respect to the claims for which trial is instituted. *See Sand Revolution II, LLC v. Continental Intermodal Group–Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020). The stipulation reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

- Factor 6 favors institution in view of compelling evidence of unpatentability of the Challenged Claims.

In short, *Fintiv* factors are either neutral or weigh in favor of institution.

B. The Board should not deny under General Plastic

The '105 patent has not been challenged in any prior IPR petition, so none of the *General Plastic* discretionary institution factors apply to this Petition. *See General Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (PTAB Sept. 6, 2016) (Section II.B.4.i. precedential).

C. Advanced Bionics Test Favors Institution.

In determining whether to institute an IPR, the Board may consider whether “the same or substantially the same prior art or arguments previously were presented to the Office.” §325(d); *Advanced Bionics, LLC v. MED-EL*

Elektromedizinische Geräte GmbH, IPR2019-01469, Paper 6, 7 (PTAB Feb. 13, 2020).

Relative to the first prong of *Advanced Bionics*, Petitioner acknowledges *another* Kesanupalli reference was “previously presented to the Office.” More specifically, U.S. Patent Pub. 2011/0138450, naming Kesanupalli. The APPL-1006/Kesanupalli, relied upon herein is not the Kesanupalli ’450 publication (or counterpart thereof), although there is some overlapping disclosure. However, none of Challener, Cheng, nor Kodama were before the Office during prosecution. Therefore, under the *first prong*, neither substantially the same art nor substantially the arguments were presented to the Office. *See Thorne Research, Inc. v. Trustees of Dartmouth College*, IPR2021-00491, Paper 18 at 7-9 (PTAB Aug. 12, 2021).

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the ’105 patent are unpatentable, and requests institution of *inter partes* review.

Respectfully submitted,

Dated: January 31, 2024

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned attorney for Petitioner declares that the argument section of this Petition (Sections I, III–XI) has 13917 (less than 14,000) words, according to the word count tool in Microsoft Word™.

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service January 31, 2024

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review, including Exhibit List; Exhibits APPL1001–APPL-1017 and APPL-1019–APPL-1029; Petition’s Notice Ranking Petitions and Explaining Material Differences Between Petitions for U.S. Patent No. 11,475,105

Persons served VAN PELT, YI & JAMES LLP
1 1st ST, STE 12
LOS ALTOS, CA 94022
UNITED STATES

/David W. O'Brien/
David W. O'Brien
Lead Counsel for Petitioner
Registration No. 40,107