

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00507

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	8
VII.	REQUESTED RELIEF	9
VIII.	OVERVIEW OF CHALLENGES	9
A.	Challenged Claims	9
B.	Statutory Grounds for Challenges	10
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE..	11
A.	Ground 1: Claims 2, 4, 12, 15, 21, 23, 31, and 34 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng and Kodama.....	11
1.	Kesanupalli.....	11
2.	Cheng	13
3.	Kodama	16
4.	Combination of Kesanupalli, Cheng and Kodama	16
5.	Independent Claim 1 (base claim to challenged claims)	20
6.	Claim 2	35
7.	Claim 4.....	36
8.	Claim 12	37

9.	Claim 15	38
10.	Claims 21, 23, 31 and 34	40
B.	Ground 2: Claims 5, 6, 24 and 25 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng, Kodama and Hubner.....	42
1.	Hubner.....	42
2.	Combination of Kesanupalli, Cheng, Kodama and Hubner	44
3.	Claim 5	49
4.	Claim 6	52
5.	Claims 24 and 25.....	55
C.	Ground 3: Claims 2, 4, 12, 15, 21, 23, 31, and 34 are obvious under 35 U.S.C. §103 over Jakobsson '351 and Kodama.	55
1.	Jakobsson '351 and Kodama	55
2.	Reasons to Combine Jakobsson '351 and Kodama	55
3.	Independent Claim 1 (base claim to challenged claims)	57
4.	Claim 2	63
5.	Claim 4	64
6.	Claim 12	64
7.	Claim 15	65
8.	Claims 21, 23, 31, 34	66
D.	Ground 4: Claims 5-6 and 24-25 are obvious under 35 U.S.C. §103 over Jakobsson '351, Kodama and Hubner.....	67
1.	Hubner.....	67
2.	Combination of Jakobsson '351, Kodama and Hubner	67
3.	Claim 5	72
4.	Claim 6	72
5.	Claims 24-25	73
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	73
A.	The <i>Fintiv</i> factors favor institution.	74
B.	The Board should not deny under General Plastic.....	76

C.	<i>Advanced Bionics</i> Test Favors Institution.....	76
XI.	CONCLUSION.....	77
XII.	CERTIFICATE OF WORD COUNT	78
	CERTIFICATE OF SERVICE	79

PETITIONER’S EXHIBIT LIST

January 31, 2024

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	Reserved
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)
APPL-1030	U.S. Patent Application No. 2012/0150808 to Hubner et al. filed December 13, 2010 and published June 14, 2012 (“Hubner”)
APPL-1031	The TLS Protocol (https://www.ietf.org/rfc/rfc2246.txt), January 1999 (retrieved January 30, 2024)
APPL-1032	The Secure Sockets Layer (SSL) Protocol Version 3.0 (https://datatracker.ietf.org/doc/html/rfc6101), August 2011 (retrieved January 30, 2024)

APPL-1033	The Kerberos Network Authentication Service (VS) (https://www.ietf.org/rfc/rfc4120.txt), July 2005 (retrieved January 30, 2024)
APPL-1034	Tseitlin, Ariel, “Embracing Failure to Improve Resilience and Maximize Availability”, acmqueue The Antifragile Organization
APPL-1035	Batten et al., “pStore: A Secure Peer-to-Peer Backup System,” https://dspace.mit.edu/handle/1721.1/149321?show=full , October, 2002
APPL-1036	Varshavsky et al., “Amigo: Proximity-Based Authentication of Mobile Devices,” UbiComp 2007, LNCS 4714, pp. 253-270, 2007
APPL-1037	Chervenak, Ann & Vellanki, Vivekanand & Kurmas, Zack. (1998). Protecting File Systems: A Survey of Backup Techniques
APPL-1038	Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Sept. 2008

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 claims 2, 4-6, 12, 15, 21, 23-25, 31, and 34 (“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.

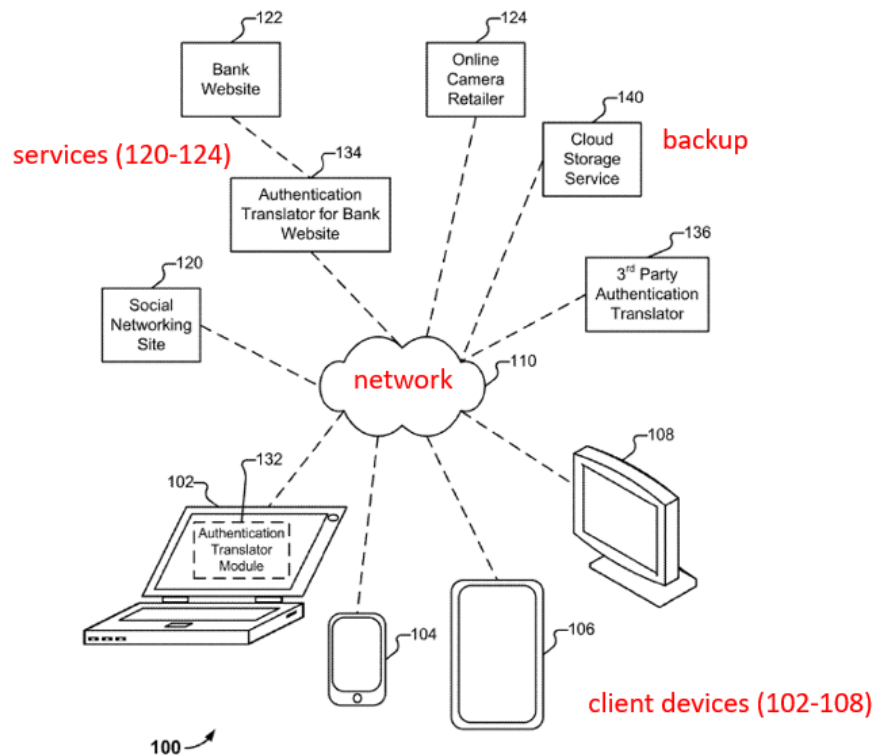
III. GROUNDS FOR STANDING

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

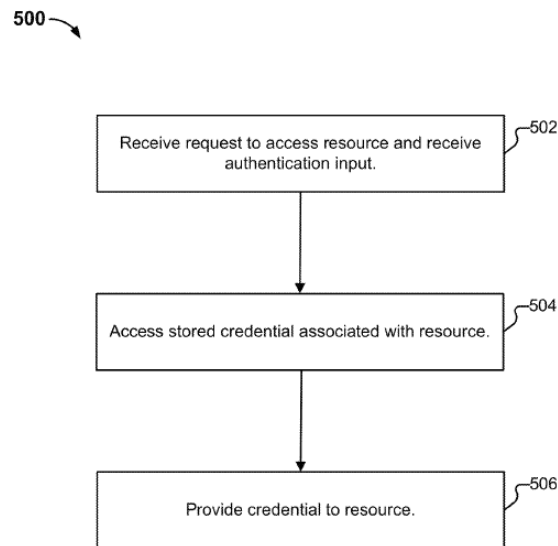
The '105 patent is directed to an environment including a client device, such as a notebook computer or tablet, which is connected via a network to a service such as a website. APPL-1001, 2:62-3:14. FIG. 1 is illustrative:



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 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, ¶¶42-61, 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 that 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).

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 of ’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). 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. *Id.* 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 Grounds 3-4 depend 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.

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

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

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.

VII. REQUESTED RELIEF

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

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 2, 4-6, 12, 15, 21, 23-25, 31, and 34 (“Challenged Claims”) of the ’105 patent are challenged.

B. Statutory Grounds² for Challenges

Grounds	Claim(s)	Basis
#1	2, 4, 12, 15, 21, 23, 31, and 34	§103 over Kesanupalli, Cheng and Kodama
#2	5-6, 24-25	§103 over Kesanupalli, Cheng, Kodama and Hubner
#3	2, 4, 12, 15, 21, 23, 31, and 34	§103 over Jakobsson '351 and Kodama
#4	5, 6, 24, 25	§103 over Jakobsson '351, Kodama and Hubner

Kesanupalli was filed March 24, 2010, published April 7, 2011, and issued August 5, 2014. Cheng was filed September 24, 2003 and published June 17, 2004. Kodama published July 15, 2009. Hubner was filed December 13, 2010 and published June 14, 2012. Kesanupalli is prior art under at least §102(a)(2); Cheng, Kodama and Hubner are prior art under at least §102(a)(1).

² As demonstrated above, the '105 patent is an AIA patent. *See supra*, IV.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), Hubner qualifies under pre-AIA §102(e), and Cheng and Kodama qualify under pre-AIA §102(b). *See also*, APPL-1003, ¶¶63-67.

Jakobsson '351 issued July 23, 2019 and qualifies as prior art under at least §102(a)(1). Only Grounds 3-4 depend on the priority date of the Challenged Claims.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 2, 4, 12, 15, 21, 23, 31, and 34 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng and Kodama.

1. Kesanupalli

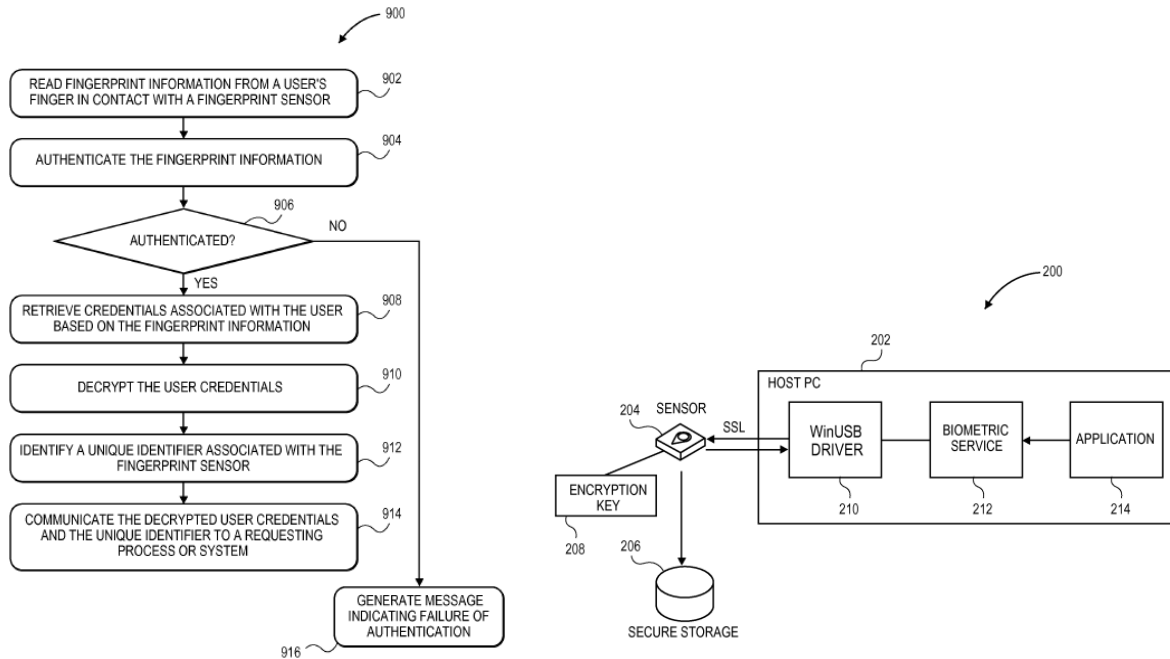
Kesanupalli is entitled “Secure User Authentication Using Biometric Information” and is directed to a secure authentication system using biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” APPL-1006, (54), 1:59-62. *See* APPL-1003, ¶¶68-73. 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, 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

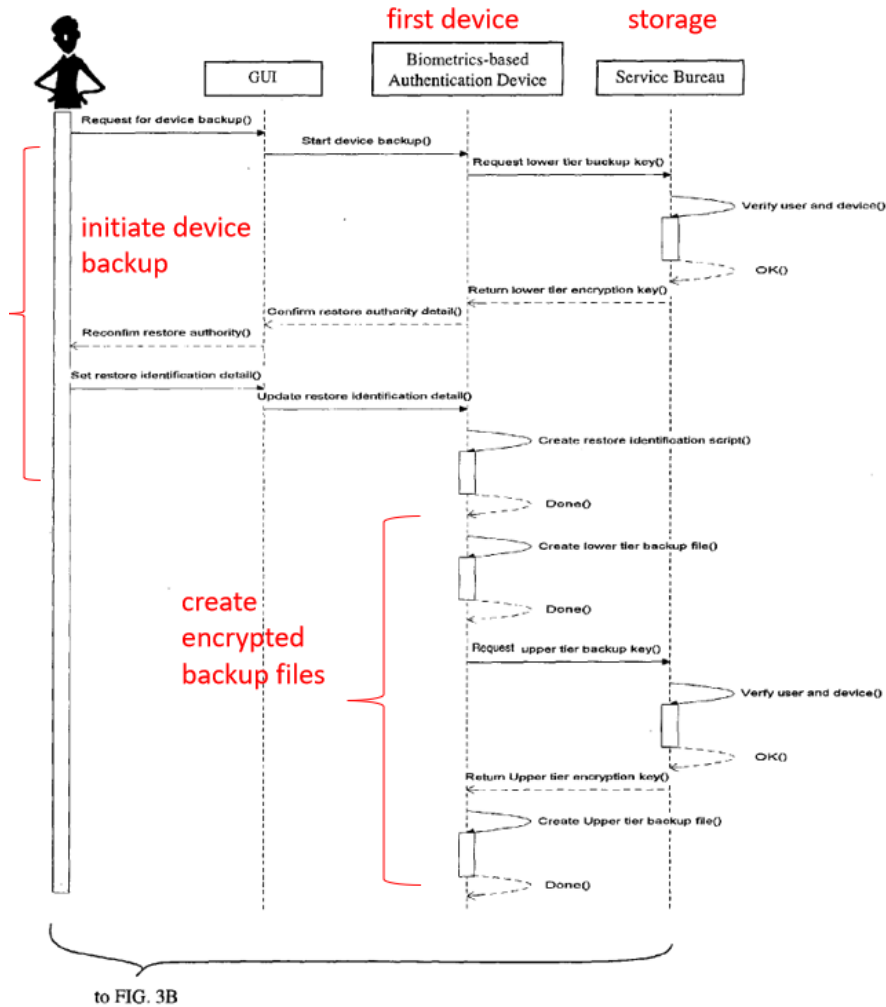
In an authentication process, sensor 204 receives a biometric input from a user and releases the user's credentials from secure storage 206 upon a successful match of the input with the user's stored biometric template. APPL-1006, 6:31-45. The released credentials are then communicated to the external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

2. Cheng

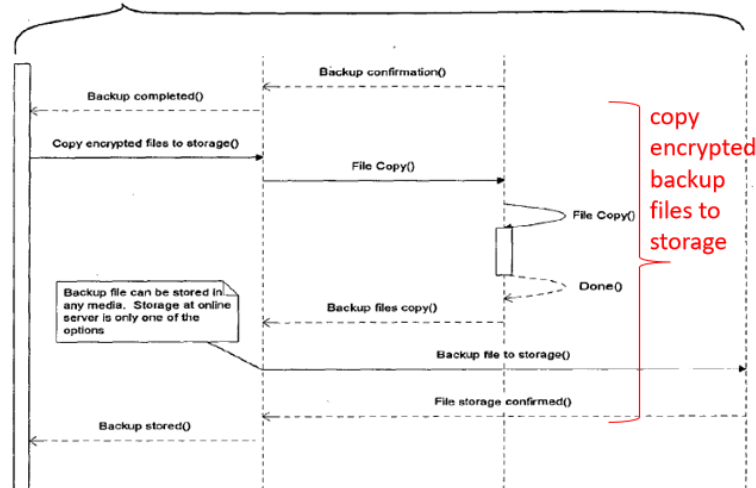
Cheng is entitled "System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information" and provides ways to "securely backup and restore" a user's authentication-based device without compromising the security thereof. APPL-1008, (54), Abstract.

Cheng recognizes "[b]iometrics-based authentication" is commonly

implemented, which leads to portable devices that 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]. Cheng’s FIGS. 3A-3B illustrate a backup of data of a user’s device 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 for backing up data. APPL-1008, [0031]-[0039].



from FIG. 3A



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

See APPL-1003, ¶¶74-77. Cheng describes a use case of a user's 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 directed to backing up data in an electronic device. APPL-1010, (57), [0040], [0041], APPL-1003, ¶¶78–80. Kodama explains its backup procedures “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].

Kodama teaches registering a first device with a backup service (storage) including “device information including the manufacturer name” and after registration, sending data to its storage. APPL-1010, [0101], [0106]–[0107]. Kodama restores data onto another device (*e.g.*, a “new” device) and to start restoration “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 the information—including the manufacturer name—of the second device coincides with the first device before permitting the backup of data to the second device. *See* APPL-1010, [0137]–[0144].

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, ¶¶81-90. 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 arising between manufacturers. *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, ¶83; *see, e.g.*, APPL-1006, 2:30-38, 2:48-50; APPL-1008, [0003]-[0004]; APPL-1001, 1:43-50, FIG. 1; APPL-1010, (57), [0040]-[0041].

Moreover, as evidenced on the front pages of Kesanupalli, the '105 patent, and Kodama, each includes the same search subclass. *See* APPL-1001, (51), (52); APPL-1006, (51) (58); APPL-1010, (51).³ POSITA would recognize it is directed

³ *see also* www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (subclass definitions);

to the same technology. APPL-1003, ¶84; APPL-1008, [0007].

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, ¶¶85-89. 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 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, ¶¶85-89; *see* APPL-1006, 10:13-18; APPL-1008, [0006]. And when introducing replacement devices,

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

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, ¶87. 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 reason to employ Kodama’s technique of controlling backup processes such that the first device and the second device (the source and target devices) are compatible. APPL, 1003, ¶89. 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, ¶89.

Finally, POSITA would have had reasonable expectations of success in

adding backup feature taught by Cheng as enhanced by Kodama in a biometric authentication system as taught by Kesanupalli because Cheng-Kodama are similarly directed to handling of personal information including biometric authentication information in a secure manner. APPL-1003, ¶¶90. 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.*

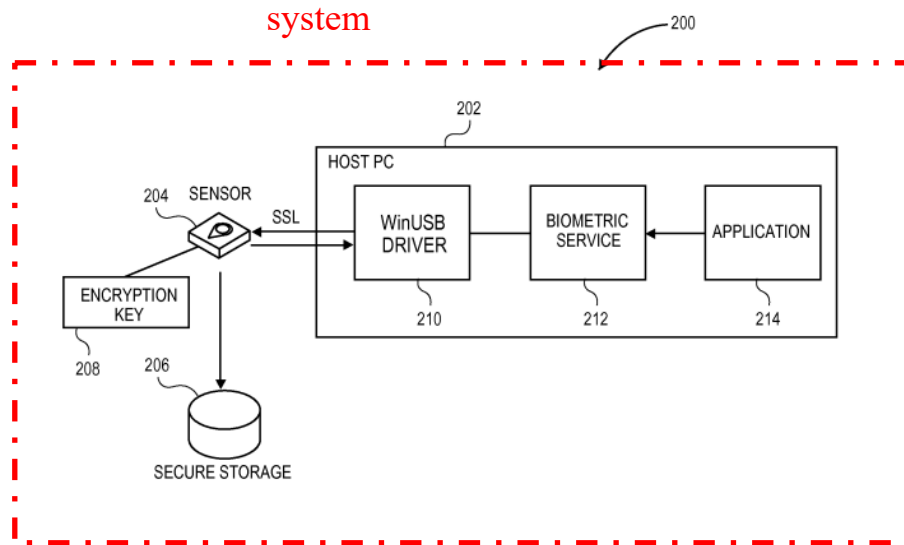
5. Independent Claim 1 (base claim to challenged claims)

[1.0] *A system, comprising:*⁴

Kesanupalli discloses *a system*. APPL-1003, ¶¶91-93.

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.

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



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.

[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, ¶¶94-97.

Kesanupalli describes what POSITA would readily recognize—namely that functions of authentication translation and communication with external resources such as discussed *supra* IX.A.1 and detailed below are performed by *one or more processors*. *Id*; APPL-1006, 9:58–10:1. The processor functions of authentication

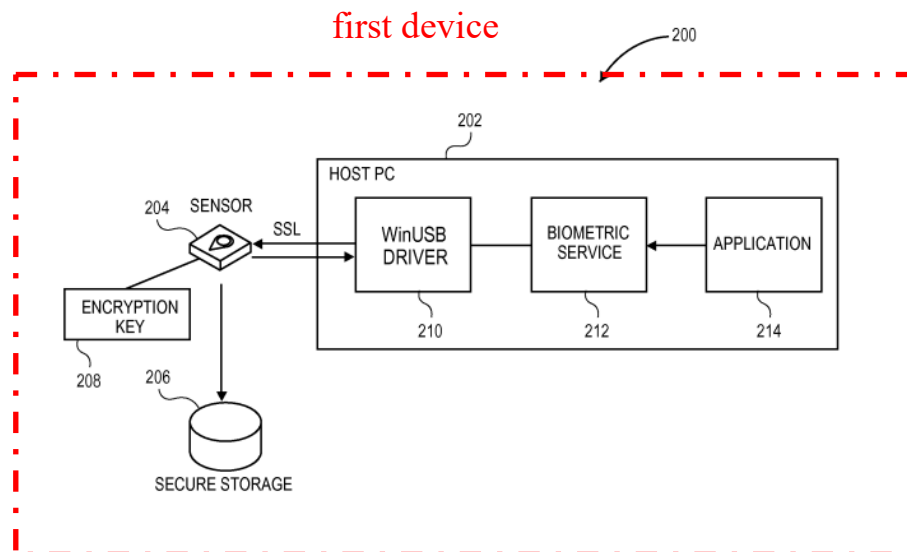
(e.g., those of sensor 204 such as matching) and the processor functions of communicating with an external resource (e.g., those of HOST PC 202) together provide *one or more processors*. See *id.*, APPL-1006, 5:62-6:31, 6:40-49.

[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, ¶¶98-106.

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, ¶¶100-102.

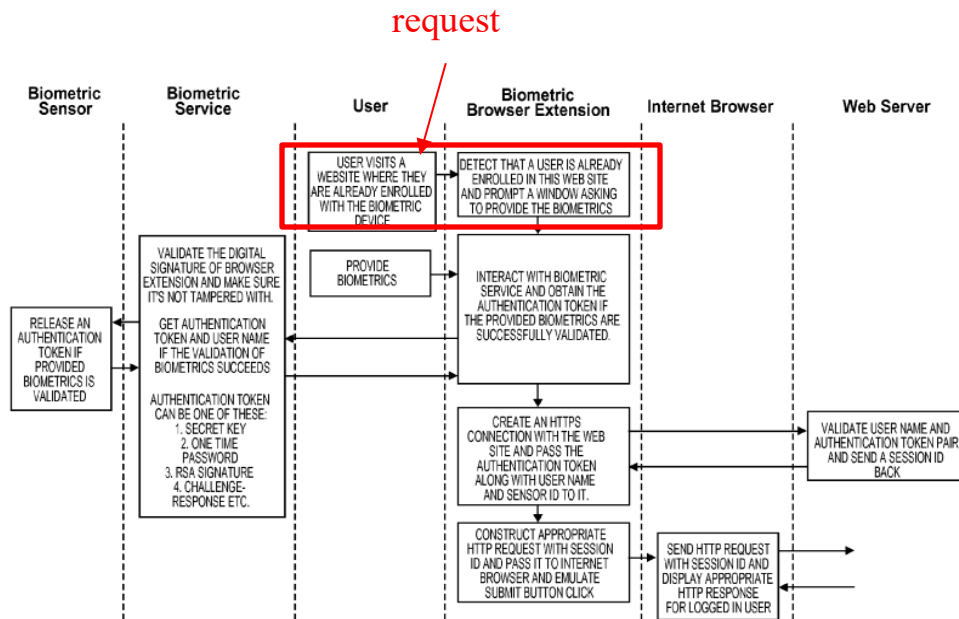


APPL-1006, FIG. 2, annotated

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, 4:3-11, 4:36-50, 6:11-49. Kesanupalli's embodiments (*e.g.*, FIG. 2) constitute a *device*. APPL-1003, ¶¶100-102; APPL-1001, 2:21-23. To the extent Patent Owner imparts some integrally-formed meaning for *device*, POSITA would understand Kesanupalli discloses this. APPL-1003, ¶102; 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 (“...secure storage device is contained within the fingerprint sensor hardware...”)

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 (“...**subsequent visits to the same Web site** cause the Web browser plug-in to detect that the user has already enrolled..., 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, ¶¶103-105.



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.

[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, ¶¶107-116.

Again Kesanupalli describes its functions are performed by one or more

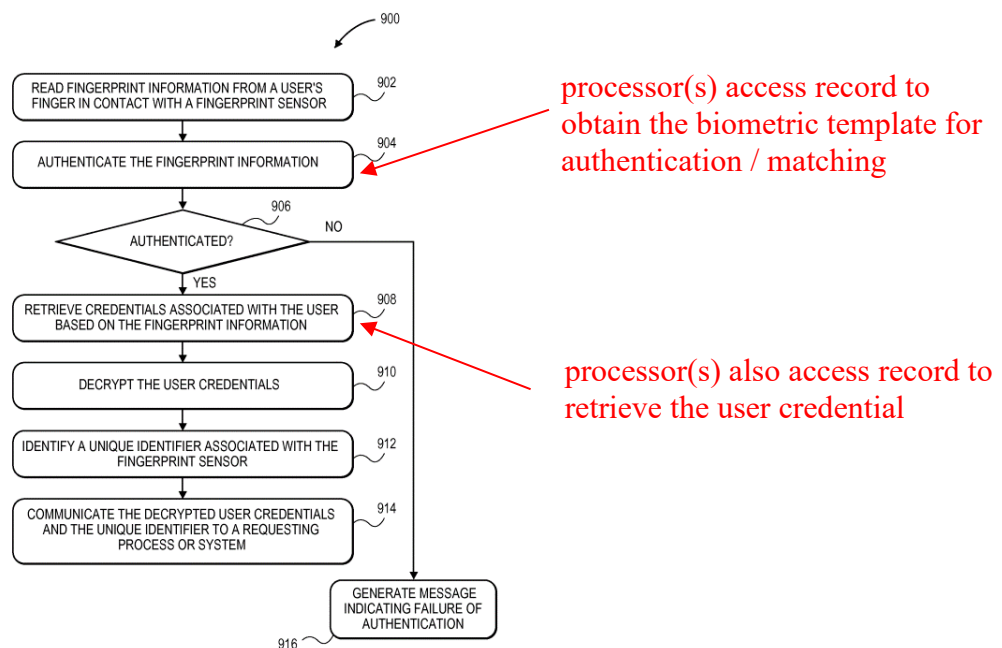
processors, which includes the functionality of limitation [1.3a].

Kesanupalli describes a user's enrollment process in an external resource (website) where the user's *credential* (key) and *authentication information* (fingerprint template) associated with the user and the website are bound and stored in the first device (in secure storage 206). APPL-1006, 3:32-51 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, ¶¶43-51.

The user's credential bound with authentication information (biometric template) is a *record*, which is *stored on the first device* in a secure storage. APPL-1003, ¶¶111-112, APPL-1019 (defining 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 is *authentication information associated with the user* as it is the user's personal biometric data. APPL-1003, ¶110.

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. 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. FIG. 9 is illustrative of authenticating a user after she has enrolled in a website and accessing the record performed by the one or more processors. APPL-1006, 8:54-56.



APPL-1006, FIG. 9, annotated

APPL-1003, ¶¶113-114. In the authentication process through FIG. 2, 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, FIGS. 2, 12, 3:44-51, 6:42-49.

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

Kesanupalli discloses this limitation. APPL-1003, ¶¶117-119.

As discussed in [1.3a], Kesanupalli describes *credential information*, which it describes as “user credentials,” exemplified by a *cryptographic key*. APPL-1006, 3:32-51 (“password, **cryptographic key**, random seed, and the like.”), 3:65-4:1, 8:6-22, FIG. 12, APPL-1003, ¶¶46-54.

[1.4] receive authentication input from the user;

Kesanupalli discloses this limitation. APPL-1003, ¶¶120-122.

As discussed above, one or more processors perform Kesanupalli’s functions, which include functionality of limitation [1.4].

Kesanupalli describes one or more processors *receive an authentication input* (e.g., biometric input) *from the user*. Kesanupalli describes sensor (204) circuitry 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 (“...**procedure 900 reads fingerprint information from a user’s finger in contact with a fingerprint sensor (902).**”), 8:54-9:3, FIG. 12

“provide[s] biometrics.”). Kesanupalli also describes other types of authentication input from the user. APPL-1006, 2:30-38.

[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, ¶¶123-126.

As discussed, one or more processors perform Kesanupalli’s functions, which includes the functionality of limitation [1.5].

Kesanupalli describes its one or more processors (executing functions of sensor 204) *determine[s] the authentication input from the user (fingerprint information) 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, ¶124; APPL-1006, 3:32-51. Kesanupalli describes the processor executing functions of sensor 204 performs the matching. APPL-1006, 6:31-49; *see also*, FIG. 2, 3:52-4:2, 5:9-24, 8:59-9:24, FIG. 12.

[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, ¶¶127-130.

As discussed, one or more processors perform Kesanupalli’s functions, which includes the functionality of limitation [1.6].

As discussed in [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 so it can be transmitted to a requesting resource (website). APPL-1006, 9:14-20 (“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 sends it to the requesting service. 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.

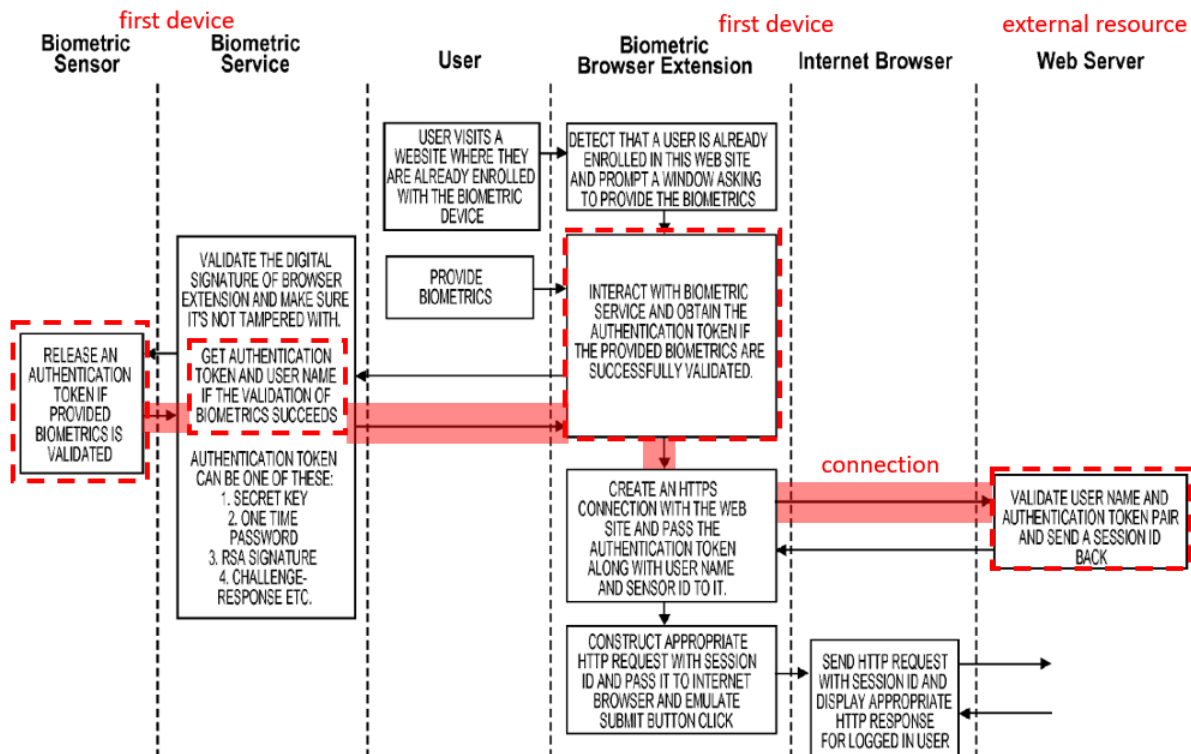
[1.7] facilitate access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device 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, ¶¶131-138.

As discussed, one or more processors perform Kesanupalli’s functions, which includes the functionality of limitation [1.7].

In Kesanupalli’s device, the 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* (from 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. APPL-1006, 9:4-24 (“...the procedure **retrieves credentials** associated with the user based on the fingerprint information...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 and PC 202 communicates it to the external resource. APPL-1006, 6:11-49. FIG. 12 is illustrative:



APPL-1006, FIG. 12, annotated

APPL-1003, ¶134. 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, 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) because the credential is used to login the user to the external resource. APPL-1003, ¶¶135-136; APPL-1006, FIG. 12 (“logged in user”), 5:22-24 (“to the Web site to complete the user authentication process”). Processor 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. Thus, 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*.

[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, ¶¶139-148.

As discussed, one or more processors perform Kesanupalli's functions and the one or more processors are *operable* and suitable to perform instructions of the functions of Kesanupalli and Cheng/Kodama's backup techniques. APPL-1003,

¶140. Cheng and Kodama confirm one or more processors execute their functions. APPL-1008, [0022]; APPL-1010, [0037].

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, ¶¶141-144. 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* by registering a first device with a storage location, such as a user service bureau, generating a "backup file(s)" of the device's data, and providing the backup file from the first device to the user service bureau (storage). *See* APPL-1008, Abstract, [0002], [0007]-[0008], [0023]-[0030], FIGS. 3A-3B. Cheng describes exemplary data for backup 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, ¶142; APPL-1008 [0007]-[0008], [0030], FIGS. 3A-3B.

Cheng's backup procedure provides the backup data from the storage location (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, ¶144, 85-89. 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, ¶¶145-147. 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 the 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 “the **manufacturer name.**” APPL-1010, [0101], [0103]. POSITA would understand “manufacturer name” to constitute a *brand* of the first device. APPL-1003, ¶146. *See also*,

APPL-1010, [0078]–[0104] (service registration), FIG. 4 (“manufacturer name 0403”), [0054], FIG. 6, [0061]. Kodama continues the backup process by sending a copy of the data of the registered first device to the backup service. APPL-1010, [0106]–[0118].

Kodama continues its backup procedure 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 by 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, ¶147. 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, ¶¶149-152.

Kesanupalli's system includes a main memory, a *memory*. APPL-1006, 10:26-47. 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, ¶151, APPL-1006, 5:59-66.

Therefore, base independent claim 1 is obvious over Kesanupalli, Cheng and Kodama. APPL-1003, ¶153.

6. Claim 2

[2.0] The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

Kesanupalli, Cheng and Kodama render obvious claim 1 and Kesanupalli discloses this further limitation. APPL-1003, ¶¶154-156.

As illustrated above, Kesanupalli describes a user device implements an authentication technique to authenticate a user to one or more external resources (web sites). *See* limitations [1.4]-[1.8]. A *second device*, *e.g.*, a user device of the

same brand as the first device, would perform authentication to an external resource using the same functionality as discussed above and as taught in Kesanupalli. APPL-1006, 2:39-64, FIGS. 2, 7, 9, 11-12.

Therefore, claim 2 is rendered obvious by Kesanupalli, Cheng and Kodama.

7. Claim 4

[4.0] The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.

Kesanupalli, Cheng and Kodama render obvious claim 1 and Kesanupalli and Cheng render obvious this further limitation. APPL-1003, ¶¶157-159.

As illustrated above, Cheng describes a backup technique where a *first device* establishes a connection with a user service bureau, which provides a storage service for the first device's data, and a *second device* establishes a connection with this bureau to download a backup file of the data. *See* limitation [1.8]. Cheng describes the devices are connected with the bureau by a "secure connection." APPL-1008, [0022] ("[o]nboard **microprocessor** and communication means [] handle communication... such as establishing a **secure connection** with a remote service bureau, requesting [] keys, creating and copying [] backup files, and terminating the connection.") Cheng describes "[a] **new biometrics-based authentication device** [*second 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). A secure connection is a *secure channel*. APPL-1003, ¶158 (describing a secure channel).

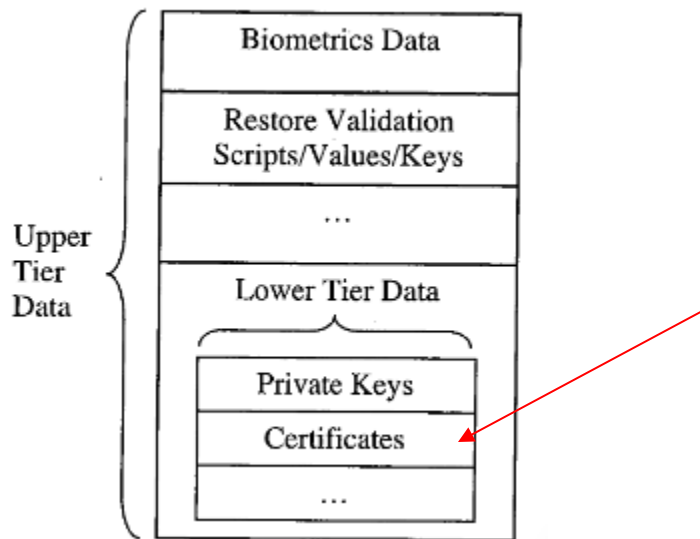
Therefore, claim 4 is rendered obvious by Kesanupalli, Cheng and Kodama.

8. Claim 12

[12.0] The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.

Kesanupalli, Cheng and Kodama render obvious claim 1 and Cheng discloses this further limitation. APPL-1003, ¶¶160-164.

Cheng’s backup procedure implemented on Kesanupalli’s system provides for encrypted backup files to be *transmitted to a second device*. *See* limitation [1.8]. Cheng also discloses the transmitted data includes a *certificate*. APPL-1008, Abstract (“The lower tier data contain encrypted electronic identity of a user and authentication information associated therewith such as private keys and **corresponding certificates.**”), [0008], [0015]. FIG. 1 of Cheng is illustrative:



APPL-1008, FIG. 1

Further, POSITA would recognize use of a certificate in cryptographic procedures such as described in Kesanupalli and Cheng (*e.g.*, encryption and decryption) typically use a certificate containing a key that can encrypt or decrypt the files. APPL-1003, ¶163 (discussing SSL protocol).

Therefore, claim 12 is rendered obvious by Kesanupalli, Cheng and Kodama.

9. Claim 15

[15.0] The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.

Kesanupalli, Cheng and Kodama render obvious claim 1 and Kesanupalli and Cheng render obvious this limitation. APPL-1003, ¶¶165-169.

The '105 patent does not define a “vault” but describes this feature as “authentication information” of a user that can include information such as

“service provider/domain, a user name, and a credential.” APPL-1001, 4:9-21, FIG. 2.

Kesanupalli describes storing a credential and a biometric template as a *record*. See limitation [1.3]. POSITA would recognize this data together with other associated information suggested by Kesanupalli (*e.g.*, user name, web site address) provides a *vault*. APPL-1003, ¶¶166-168. In particular, Kesanupalli illustrates at enrollment a user’s “Application ID[,] **User ID**[,] User Credential” along with the biometric data are provided for storage. APPL-1006, FIG. 3, 6:50-67. Further, “[t]he **address or location information** [of the external resource/web site] is stored within the user credentials and is established as part of the enrollment process.” APPL-1006, 4:9-11. “User credentials and **other information** may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism.” APPL-1006, 6:47-49. Thus, Kesanupalli describes storing in secure storage 206, a *vault* including, *e.g.*, biometric template, credential, user ID, and an address for the associated external resource. APPL-1003, ¶¶167-168. As Dr. McDaniel explains, a vault (such as that which Kesanupalli stores in secure storage 206) includes all of the security information that makes up the repository, including the ciphertext, an encrypted initialization vector, etc., and when copied to a different device, data will be encrypted with a different set of keys. *Id.* Accordingly, POSITA would expect the version of the vault copied to a

second device to be *modified* at least in that ciphertext and initialization vectors would be changed. *Id.*

Moreover, versioning and credential usage tracking were routine for replicated data repositories and authentication databases such that POSITA would expect modifications on copying. APPL-1003, ¶168. Finally, in Kesanupalli-Cheng-Kodama system, this data of the first device (a *vault*), is copied and encrypted in a two-tier encryption of Cheng for transmitting to a second device (via the user service bureau). *See* limitation [1.8]. The backup copy provided to the second device is *modified* in this manner as well from that stored in the first device as it is encrypted by Cheng’s two-tier encryption technique. APPL-1008, FIGS. 3A-3B. Therefore, Kesanupalli and Cheng describe a *backup comprises copying a modified version of a vault to the second device*.

Therefore, claim 15 is rendered obvious by Kesanupalli, Cheng and Kodama.

10. Claims 21, 23, 31 and 34

Claims 21, 23, 31 and 34 are obvious over Kesanupalli, Cheng and Kodama. APPL-1003, ¶¶170-173. Claim 18 is the basis for these dependent claims, and the limitations of base independent claim 18, except its preamble, are substantively identical to claim 1’s limitations, as correlated in the table below:

Claim 18	Corresponding Limitation illustrating
----------	--

	obviousness over 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 render it obvious. The citations in the analysis above apply to a *system* of claim 1 and also to a *method*. APPL-1003, ¶171; 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 rendered obvious by Kesanupalli, Cheng and Kodama.

Dependent claims 21, 23, 31, and 34 are substantively identical to limitations discussed above, except that they depend from method claim 18 and thus are rendered obvious for the same reasons. APPL-1003, ¶173.

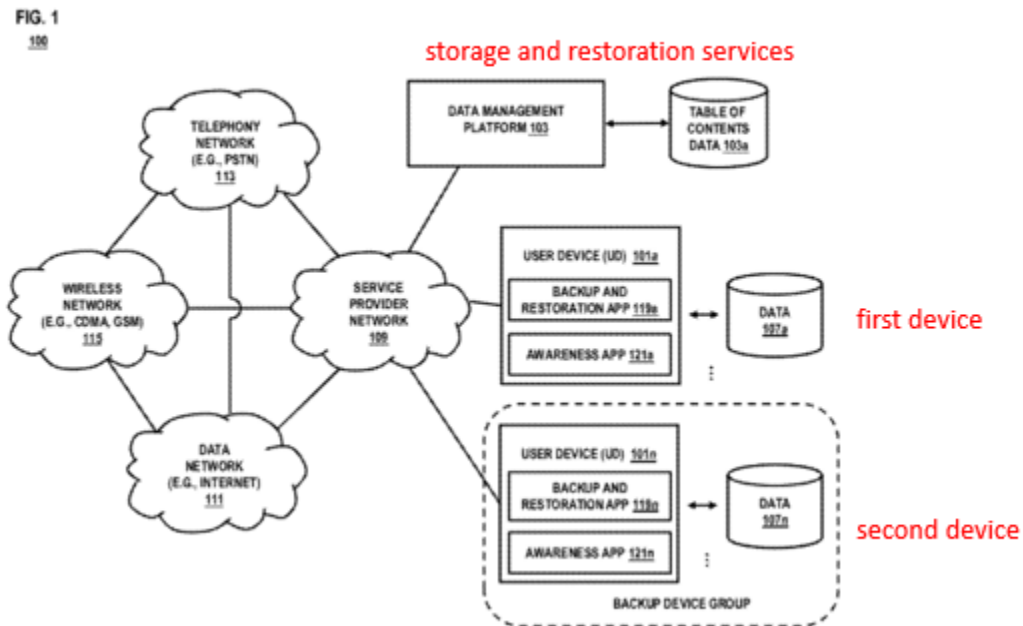
'105 Patent Claim	Corresponding limitation illustrating obviousness over Kesanupalli, Cheng and Kodama
21	[2.0]
23	[4.0]
31	[12.0]
34	[15.0]

B. Ground 2: Claims 5, 6, 24 and 25 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng, Kodama and Hubner.

1. Hubner

Hubner provides “[a]n approach for enabling execution of data backup and restoration among a group of user devices” and, in particular between “peer

devices” over wireless communications. APPL-1030, (54), (57). *See also*, APPL-1003, ¶174. FIG. 1 illustrates a system having a plurality of user devices (*e.g.*, mobile phone, laptop) and a data management platform, which provides “backup and restoration services to these devices 101a-101n,” connected by a network. APPL-1030, [0012]. While Hubner includes backup techniques that store copies of user device data in network-based storage (*e.g.*, online storage), it also recognizes limitations of such an approach and also provides backup and restoration between in-range pairs of devices using peer-to-peer communications and in-range presence detection techniques. *See* APPL-1030, [0012], [0017]. Hubner “facilitate[s] the data restoration process based on the established physical presence of the user devices.” APPL-1030, [0015]. When a source device belonging to a device backup group is in proximity of a peer device, backup or restoration of the data to the peer device is initiated. APPL-1030, [0015]-[0017], [0021]. Hubner’s local presence awareness and backup/restore techniques use peer-to-peer communication such as Bluetooth or other near-field communication. APPL-1030, [0017], [0026].



APPL-1030, FIG. 1, annotated

2. Combination of Kesanupalli, Cheng, Kodama and Hubner

POSITA would have been motivated to apply Hubner's teachings of backing up data using peer-to-peer techniques to Kesanupalli's system as enhanced by Cheng and Kodama. APPL-1003, ¶¶175-180. Kesanupalli's system having Cheng-Kodama's backup technique applied along with peer-to-peer techniques of Hubner would produce obvious, beneficial, and predictable results of enabling the backup and/or restoration of data to/from a physically-proximate, qualified peer device, increasing the opportunity for backup and restoration of data thereby increasing the likelihood of the availability of the data in the event of damage or loss of the data on a first device. See APPL-1030, [0001], [0012]. The increased the opportunity for backup and restoration is particularly significant when/where

wide-area network (WAN) communications may be unavailable or bandwidth limited. APPL-1003, ¶176.

First, Hubner is in the same field of endeavor as Kesanupalli, Cheng, Kodama and the '105 patent, such as security arrangements and procedures for transferring and protecting data in computer systems. *See supra* IX.A.4; APPL-1003, ¶176; APPL-1030, [0012], FIG. 1 “system 100” having user devices, network connections, FIG. 6, FIG. 2 “authentication module,” [0027], [0030]-[0031]. Hubner also would have been reasonably pertinent to a problem faced by the inventor of the '105 patent—providing **options** in a system for backing up data, which mitigates reliance on a particular backup technique. *See* APPL-1001, 11:54-12:3, 12:65-13:3, 14:23-25; APPL-1030, [0012]-[0015]. POSITA would be motivated to improve system designs, such as those relying on network connections as in the '105 patent and Kesanupalli/Cheng/Kodama, to consider independent failure modes—engineering such improved designs to implement multiple independent channels to improve resilience. APPL-1003, ¶176.

Second, POSITA would have been motivated to employ Hubner’s peer-to-peer technique of backing up and restoring data in connection with Kesanupalli having Cheng-Kodama’s backup technique applied to provide a user or system with a benefit of additional opportunities for backing up data of a user device. APPL-1003, ¶¶176-179. Just as discussed in Section IX.A.4 with respect to the

Kesanupalli/Cheng/Kodama combination, Hubner recognizes what POSITA would understand—that data backup and restoration techniques are “required for various reasons, including data loss, file corruption[,], computing system failure[,],” including due to device damage or loss. APPL-1030, [0001], [0012]; APPL-1006, 10:13-18; APPL-1008, [0006]. However, users may not diligently back up data. Therefore, additional modes of “effective, convenient execution of data backup and restoration for user devices” are beneficial. APPL-1030, [0001]-[0002], [0012].

POSITA would recognize benefits in applying Hubner’s peer-to-peer backup technique as it provides optionality in backup techniques within a system, which can increase the likelihood of a successful backup and restoration. APPL-1003, ¶¶176-179. Adding peer-to-peer communications allows for backup data transfer that avoids a bottleneck at, or unavailability of, a WAN interface. *Id.* One particular option provided by Hubner’s procedure of backing up and restoring data is use of local communication techniques between in-range, peer devices. Cheng suggests its backup procedure uses “public networks such as the internet” for connection between user devices and the user service bureau (storage service). *See*, APPL-1008, [0029]; *see also*, APPL-1006, 1:27-34. POSITA would recognize limitations of public network technology (e.g., a wide-area network (WAN)), for example, instances of WAN-connectivity being unavailable, having

limited bandwidth, being metered, or being otherwise costly to the user. APPL-1003, ¶178. Hubner's peer-to-peer technique facilitates backup and restoration to/from in-range peer devices even when public network connectivity is limited. APPL-1030, [0017], [0026] (discussing e.g., Bluetooth connectivity).

Third, another benefit POSITA would recognize in applying Hubner's technique of communicating data between peer-level devices is an increase in security. APPL-1003, ¶179. In Hubner's techniques, communication of data is based on proximity detection between peer devices previously registered and established as a device group using traditional authentication techniques. POSITA would appreciate that Hubner's awareness of physical proximity of peer devices communicating using near-field techniques can be employed as an additional factor in a multifactor authentication scheme to increase confidence in authentication of a target device or system. *Id.*; *see, e.g.*, APPL-1030, awareness application 121, [0016], [0017]. Further, this proximity detection provides yet another benefit of “**automatically** facilitat[ing] the data restoration process based on the established physical presence of the user device[.]” mitigating a need for user to manually initiate the restoration. APPL-1030, [0015].

Finally, POSITA would have had reasonable expectations of success in adding a peer-to-peer backup feature such as taught by Hubner to the system of Kesanupalli with Cheng-Kodama's backup techniques. Hubner invites

combination with other backup techniques: “Regardless of the approach employed, data backup may be performed due to data loss, file corruption, computing system failure or the like. These techniques can be employed **in conjunction with the peer-distributed**, network-controlled data backup and restoration services of platform 103.” APPL-1030, [0013]. Moreover, Hubner applies to “data of all types” and is directed to substantially similar user devices interacting with a data management platform over a network that is just like the service bureau of Cheng. APPL-1003, ¶180; APPL-1030, [0014], [0022], [0023], FIG. 1. Adding peer-to-peer communications feature for backup/restore would merely have been applying a known technique to a known device (method, or product) 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. APPL-1003, ¶180. Further, POSITA would have had an expectation of success as the teachings of Kodama provide for mitigating compatibility issues between the peer-to-peer exchange by ensuring the peer devices are a same brand. *Id.*

3. Claim 5

[5.0]. *The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.*

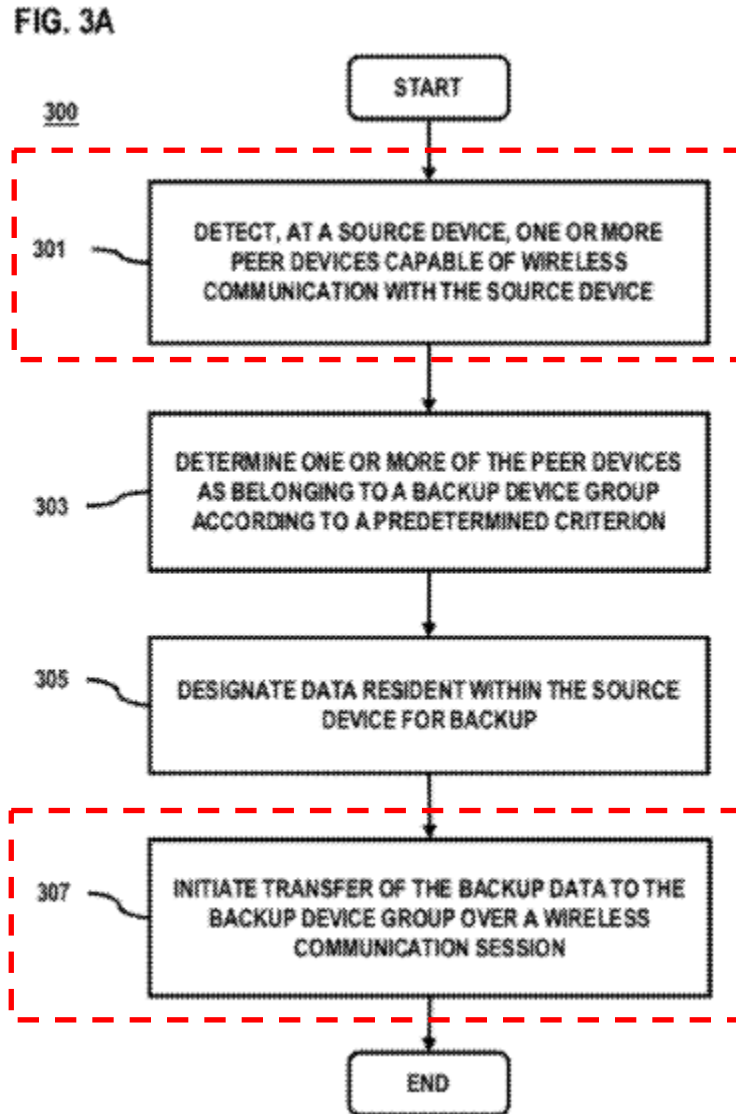
Claim 1 is rendered obvious by Kesanupalli, Cheng, and Kodama as discussed above; claim 5 is rendered obvious by Kesanupalli, Cheng, and Kodama and also in further view of Hubner. APPL-1003, ¶¶181-187.

Claim 5 recites the first and second devices are *configured to complete a pairing process*. Note that the claim does not expressly require that the first device pairs **with** the second device. The '105 patent does not define “pairing” but includes an example of “pairing” between a user device “and an external resource” such as “cloud storage,” where the pairing includes the user device sending “a certificate or another type of assurance” to the external resource before data is transmitted to the device. APPL-1001, 16:33-49; APPL-1003, ¶185 (explaining the '105 patent's inclusion of conventional cloud storage within its concept of “pairing”). This is the same procedure as disclosed in Cheng which, in view of the '105 patent example, describes devices *configured to complete a pairing process* as illustrated in FIG. 4A, where a user device initializes with the service bureau, shares keys, and the target data. *See* APPL-1008, FIG. 4A, [0032]-[0035]. It would have been obvious for both the first device and the second device to be configured to include this functionality in order to facilitate their interactions with a backup service as taught by Cheng. APPL-1003, ¶182.

To the extent the Patent Owner argues that the *pairing process* of claim 5 is directed to pairing **between** user devices (i.e., peer-to-peer), it would have been obvious to configure the first and second devices of Kesanupalli-Cheng-Kodama to perform this function using near-field, Bluetooth or other peer-to-peer communication and/or local presence detection techniques as taught by Hubner.

Hubner describes techniques providing for a *first device* and a *second device* to be *configured to complete a pairing process*. Hubner describes a source device (a *first device*) and a backup device (a *second device*) in its user devices 101a-101n, which can communicate data with one another (e.g., for the purposes of backup and synchronization of data) using near-field or short-range communication signals such as Bluetooth, which involves a *pairing process* by which peers register with each other. APPL-1003, ¶¶ 183-185 (explaining Bluetooth pairing in context). “In one embodiment, when one or more **peer user devices 101a-101n** are registered...[and] are **detected as being within range of one another**, the data management platform 103 causes one or more of them to initiate backup of data stored in respective memory 107a-107n to the other peer devices 101a-101n...the various signals detected by the integrated sensory systems of the peer user devices 101a-101n, including **Bluetooth signals**” APPL-1030, [0017]. *See also*, [0026], [0031].

FIGS. 3A-3D of Hubner illustrate pairing implemented by user devices, representative portion FIG. 3A is reproduced below:



APPL-1030, FIG. 3A

APPL-1030, [0036] (discussing synchronization between devices), [0038]-[0039].

Thus, Hubner describes *the first device and the second device are configured to complete a pairing process*, which would have been obvious to provide to the

first and second devices of the Kesanupalli as modified by Cheng and Kodama system. APPL-1003, ¶¶184-185; APPL-1030, [0013].

Therefore, claim 5 is rendered obvious by Kesanupalli, Cheng, Kodama and Hubner.

4. Claim 6

6. *The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.*

Claim 5 is rendered obvious by Kesanupalli, Cheng, and Kodama and by Kesanupalli, Cheng, Kodama and Hubner as discussed above, which also render obvious limitations of claim 6. APPL-1003, ¶¶188-192.

As to the *pairing process* as described with respect to Cheng's backup procedure, Cheng describes a user device targeting for restoring data "needs to enroll the relevant biometrics in the new device." APPL-1008, [0009]. POSITA would understand Cheng's registration process for a user device with the backup service involves performing user authentication to gain "access clearance," which enables access to the keys used for accessing the restored data. APPL-1003, ¶189 (citing APPL-1008, [0009]). Authentication requires comparison of data to securely identify the user, e.g., matching biometric data in biometric authentication, or comparing a hash of a password (which is data generated from authentication input of a user password).

To the extent the pairing processing of claim 6 is directed to a peer-to-peer pairing as discussed in claim 5, Hubner describes its peer-to-peer backup process (a *pairing process*) requires each of the source device and the backup device be registered with a data management platform that supervises the backup processes; the registration data includes “a registration identifier, user name and identifier, device name and type, device identifier, data sharing preferences, service level preferences, etc.” APPL-1030, [0016]. Further, Hubner’s data management platform includes an authentication module 201 that “authenticates users and user devices 101a-10 n for interaction with the data management platform 103.” APPL-1030, [0030], FIG. 2. “Authentication may include **receiving and validating a login name and/or user identification value** as provided or established for a particular user during a subscription or registration process with the service provider. The login name and/or user identification value may be received as input provided by the user by way of the user device 101[.]” APPL-1030, [0031]. POSITA would understand validating a login name or identification value includes a comparison of data generated from one or more authentication inputs (*e.g.*, the user name or user identification value) to that received at the user’s enrollment; this is simply the function of authenticating a user to the system. APPL-1003, ¶190. It is noted Hubner’s inputs for enrollment/authentication are the same as the *authentication inputs* discussed in the ’105 patent. APPL-1001, 20:67-21:5 (“user

input, such as a fingerprint, iris biometric information, face biometric information, or another input with the capability to authenticate the user, including other biometric information and/or a password, **PIN** or knowledge-based authentication string. Such user input is referred to herein as authentication input.”) Moreover, POSITA would have understood that Bluetooth own pairing process (one of the near-field communication technologies employed in Hubner) includes comparison of data generated from one or more authentication inputs. APPL-1003, ¶190 (explaining authentication inputs in various Bluetooth security modes).

To the extent that the Patent Owner argues *authentication input* is a biometric input and *comparison* is a comparison of biometric input with a biometric template, implementing a biometric authentication would have been obvious in light of Kesanupalli. Kesanupalli cautions against authentication techniques based on factors such as a user name or password, and presents biometric authentication techniques. *See* APPL-1006, 1:35-46, 2:30-48, FIGS. 7, 9. POSITA would have reason to increase the security of Hubner’s pairing process by enhancing the validation of the user by biometric authentication (e.g., using biometric input, which the authentication module of the platform compares to later user input to authenticate a user) for registration of the device in a pairing process. APPL-1003, ¶191.

Thus, claim 6 is obvious over Kesanupalli, Cheng, Kodama and Hubner.

5. Claims 24 and 25

Dependent claims 24-25 are substantively identical limitations to claims 5-6 already addressed above but depend from method Claim 18. The combination of Kesanupalli, Cheng Kodama, and Hubner renders obvious these claims for the same reasons as discussed above with respect to Claims 5-6 and 18. APPL-1003, ¶193.

C. Ground 3: Claims 2, 4, 12, 15, 21, 23, 31, and 34 are obvious under 35 U.S.C. §103 over Jakobsson '351 and Kodama.

1. Jakobsson '351 and Kodama

Jakobsson '351 is a patent stemming from U.S. Application No. 15/042,636, which the '105 patent claims priority to (through a CIP). Jakobsson '351 does not contain written description of the Challenged Claims of the '105 patent as it at least 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, ¶¶38-41, 194. Kodama discloses this limitation which would be obvious to combine with Jakobsson '351; Kodama is discussed *supra* IX.A.3. APPL-1003, ¶¶78-80.

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 Jakobsson '351's backup technique are of the same brand, which provides the

obvious, beneficial and predictable result of mitigating compatibility or security issues that may arise between brand differences when transferring data. APPL-1003, ¶¶195-198.

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, ¶196; 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, ¶197. Jakobsson '351 describes the desire to back up or synchronize data across a user's devices. APPL-1011, 7:37-41. 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, ¶197. Kodama also describes its system “mitigat[es] 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 had reasonable expectations of success in applying Kodama’s teachings. APPL-1003, ¶198. “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, ¶198.

3. Independent Claim 1 (base claim to challenged claims)

[1.0] A system, comprising:

Jakobsson ’351 provides *a system*, which is summarized in its claim 1. APPL-1003, ¶¶199-200; APPL-1011, 10:50 (“1. A system, comprising:”). As

described below, Jakobsson '351's claim 1 provides, except for the backup initiating, substantially similar limitations as those of claim 1 of the '105 patent.

[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 describes this limitation. APPL-1003, ¶¶201-202.

[1.2] receive...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 describes this limitation. APPL-1003, ¶¶203-204.

[1.3a] access...

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

Jakobsson '351 claim 1 discloses:

...in response to determining...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 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 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 describes this limitation. APPL-1003, ¶¶205-208.

[1.4] receive authentication input from the user;

[1.5] determine... first device;

Jakobsson '351 claim 1 also discloses 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. And “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 [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 describes these limitations. APPL-1003, ¶¶209-212.

[1.6] retrieve...device;

Jakobsson ’351 claim 1 further discloses one or more processors “**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, ¶¶213-214.

[1.7] facilitate...user; and

Jakobsson ’351 discloses one or more processors “**...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 [] retrieved from the record ...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 describes this limitation. APPL-1003, ¶¶215-216.

[1.8] *based ...record; and*

Jakobsson '351 and Kodama render obvious this limitation. APPL-1003, ¶¶217-223.

Jakobsson '351 recites its processors are configured to “encrypt [] 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 *supra* IX.A.3, IX.A.5,[1.8], Kodama teaches registering a first device with a backup service explaining this registration includes device information of a *brand* (e.g., manufacturer name). See APPL-1010, [0101], [0103]; APPL-1003, ¶¶221-222. See also, APPL-1010 [0078]–[0104], FIG. 4, [0054], FIG. 6, [0061]. Kodama then continues the backup process by sending a

copy of the data of the first device 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 registers a *second device* (e.g., a “new” device) associated with the backup service. APPL-1010, [0160], [0157], [0137]. The registration includes providing “[*second*] device information including the manufacturer name, model name and product serial number.” APPL-1010, [0135]–[0136]. The backup service system “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 *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 to apply Kodama’s teaching to Jakobsson ’351’s system for at least the compatibility reasons described in Kodama.

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

[1.9] a memory...with instructions.

Jakobsson '351 claim 1 discloses 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, ¶¶224-225.

Therefore, the limitations of base claim 1 are obvious over Jakobsson '351 and Kodama. APPL-1003, ¶226.

4. Claim 2

[2.0] The system of claim 1, wherein the second device is used to authenticate the user to one or more external resources.

Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation. APPL-1003, ¶¶227-229.

As illustrated above, Jakobsson '351 describes a user device implements an authentication technique used to authenticate a user to one or more external resources (web sites). *See* limitations [1.4]-[1.8]. It would have been obvious for a second device in a backup technique discussed in claim 1, including a device of a same *brand*, to authenticate the user to external resources like the first device.

Therefore, claim 2 is rendered obvious by Jakobsson '351 and Kodama.

5. Claim 4

[4.0] *The system of claim 1, wherein the backup is completed after a secure channel is established by at least one of the first device and the second device.*

Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation. APPL-1003, ¶¶230-232.

Jakobsson '351 suggests a user device communicates with a storage service to keep the authentication information synchronized. APPL-1011, 8:10-12. It would have been obvious to implement a *secure channel* for this communication as Jakobsson '351 suggests the data for backup merits security protections (*e.g.*, is stored in a secure storage) and describes delivering data to another service provider using a “secure connection.” APPL-1011, 4:67-5:3 (describing a secure connection between a user device and website); APPL-1003, ¶231.

Therefore, claim 4 is rendered obvious by Jakobsson '351 and Kodama.

6. Claim 12

[12.0] *The system of claim 1, wherein the backup causes a certificate to be transmitted to the second device.*

Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and POSITA would have found it obvious to include a certificate. APPL-1003, ¶¶223-235.

Jakobsson '351 describes communicating a credential associated with a website for backup (*see* limitation [1.8]) and Jakobsson '351 further recognizes

communication between the user device and service provider is through SSL connection. APPL-1011, 5:1-3, 5:43-6:5. POSITA would recognize including a *certificate* in the authentication data associated with a website accessed by SSL would have been obvious because SSL communication includes an SSL certificate that authenticates a website's identity and enables a secure connection. APPL-1003, ¶234. It would have been obvious for the data backed up from a first device to a second device to include, along with the credential and website address, the associated website's certificate to allow the second device to communicate with the website using the SSL connection provided by Jakobsson '351. *Id.*

Therefore, claim 12 is rendered obvious by Jakobsson '351 and Kodama.

7. Claim 15

[15.0] *The system of claim 1, wherein the backup comprises copying a modified version of a vault to the second device.*

Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation. APPL-1003, ¶236-238.¶

Jakobsson '351 describes “[p]rofiles and vaults can be updated while in secure storage; if this occurs, they are encrypted and MACed before being written back to the insecure storage, which may in turn propagate them to external backup storage.” APPL-1011, 4:7-11. The updated, encrypted vault is a *modified version*, which is copied to the external backup storage during the backup procedure, and subsequently would have been obvious to download to a second device in the

backup procedure. APPL-1003, ¶237; APPL-1011, 7:2-10. Moreover, for each of the changed ciphertext and updated version tracking and usage data reasons explained relative to Ground 1, claim 15, POSITA would expect the version of the vault copied to a second device to be a *modified* version. APPL-1003, ¶237.

Therefore, claim 15 is rendered obvious by Jakobsson '351 and Kodama.

8. Claims 21, 23, 31, 34

Claims 21, 23, 31 and 34 depend from base independent claim 18, the limitations of which, except its *method* preamble, are substantively identical to limitations already addressed above. The chart below illustrates Jakobsson '351 and Kodama render claim 18 obvious. APPL-1003, ¶¶239-241.

Claim 18 Limitation (see chart in Ground 1)	Additional Disclosure of Jakobsson '351	Applicable Analysis of Claim Limitation discussed 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</i>	As to [18.7b],	[1.8]

<i>device,</i> [18.7b] <i>initiating a backup, to the second device, of at least a portion of the at least one record.</i>	14:16-22	
---	----------	--

Dependent claims 21, 23, 31, and 34 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, ¶241.

'105 Patent Claim	Corresponding limitation illustrating obviousness over Jakobsson '351 and Kodama
21	[2]
23	[4]
31	[12]
34	[15]

D. Ground 4: Claims 5-6 and 24-25 are obvious under 35 U.S.C. §103 over Jakobsson '351, Kodama and Hubner.

1. Hubner

Hubner is discussed *supra* IX.B.1.

2. Combination of Jakobsson '351, Kodama and Hubner

POSITA would have been motivated to apply Hubner's teachings of backing up data using peer-to-peer techniques to Jakobsson '351's system as

enhanced by Kodama. APPL-1003, ¶¶243-248. Jakobsson '351 device as enhanced by Kodama with peer-to-peer techniques of Hubner would produce obvious, beneficial, and predictable results of enabling the backup and/or restoration of data to/from a physically-proximate, qualified peer device, increasing a user's opportunity to backup data to ensure its availability thereby increasing the likelihood of the availability of the data in the event of damage or loss of the data on a first device. APPL-1030, [0001], [0012]. The increased the opportunity for backup and restoration is particularly significant when/where wide-area network (WAN) communications may be unavailable or bandwidth limited. APPL-1003, ¶¶243-246, POSITA would have been further motivated to apply Hubner in light of Kodama's teachings of ensuring the peer devices implementing the backup are the same brand thus mitigating device compatibility issues. *Id.*

First, Hubner is in the same field of endeavor as Jakobsson '351 as enhanced by Kodama and the '105 patent, such as security arrangements and procedures for transferring and protecting data in computer systems. *See supra* IX.C.2. (Hubner) APPL-1030, [0012], FIG. 1 "system 100," FIGS. 2, 6 "authentication module" [0027], [0030]-[0031]. Hubner also would have been reasonably pertinent to a problem faced by the inventor of the '105 patent—providing **options** in a system for backing up data, which mitigates reliance on a particular backup technique. *See* APPL-1001, 11:54-12:3, 12:65-13:3, 14:23-25;

APPL-1030, [0012]-[0015]. POSITA would be motivated to improve system designs, such as those relying on network connections as in the '105 patent and Jakobsson '351/Kodama, to consider independent failure modes—engineering such improved designs to implement multiple independent channels to improve resilience. APPL-1003, ¶¶244-246.

Second, POSITA would have been motivated to employ Hubner's peer-to-peer technique of backing up and restoring data in connection with Jakobsson '351/Kodama's backup technique applied to provide a user or system with a benefit of additional opportunities for backing up data of a user device. APPL-1003, ¶¶244-246. Just as discussed in Section IX.C.2 with respect to the Jakobsson '351/Kodama combination, Hubner recognizes what POSITA would understand—that data backup and restoration techniques are “required for various reasons, including data loss, file corruption[,] computing system failure[,]” including due to device damage or loss. APPL-1030, [0001], [0012]. However, users may not diligently back up data. Therefore, additional modes of “effective, convenient execution of data backup and restoration for user devices” are beneficial. APPL-1030, [0001]-[0002], [0012].

POSITA would recognize benefits in applying Hubner's peer-to-peer backup technique as it provides optionality in backup techniques within a system, which can increase the likelihood of a successful backup and restoration. APPL-

1003, ¶¶244-246. Adding peer-to-peer communications allows for backup data transfer that avoids a bottleneck at, or unavailability of, a WAN interface. *Id.* One particular option provided by Hubner's procedure of backing up and restoring data is use of local communication techniques between in-range, peer devices. Jakobsson '351 suggests its backup procedure uses "single network cloud 110" for connection between user devices and the cloud storage service. *See*, APPL-1011, FIG. 1, 2:25-30. POSITA would recognize limitations of public network technology (e.g., a wide-area network (WAN)), for example, instances of WAN-connectivity being unavailable, having limited bandwidth, being metered, or being otherwise costly to the user. APPL-1003, ¶246. Hubner's peer-to-peer technique facilitates backup and restoration to/from in-range peer devices even when public network connectivity is limited. APPL-1030, [0017], [0026] discussing, e.g., Bluetooth connectivity.

Third, another benefit POSITA would recognize in applying Hubner's technique of communicating data between peer-level devices is an increase in security. APPL-1003, ¶247. In Hubner's techniques, communication of data is based on proximity detection between peer devices previously registered and established as a device group using traditional authentication techniques. POSITA would appreciate Hubner's awareness of physical proximity of peer devices communicating using near-field techniques can be employed as an additional

factor in a multifactor authentication scheme to increase confidence in authentication of a target device or system. *Id.*; *see, e.g.*, APPL-1030, awareness application 121, [0016], [0017]. Further, this proximity detection provides yet another benefit of “**automatically** facilitat[ing] the data restoration process based on the established physical presence of the user device[]” mitigating a need for user to manually initiate the restoration. APPL-1030, [0015].

Finally, POSITA would have had reasonable expectations of success in adding a peer-to-peer backup feature such as taught by Hubner to the system of Jakobsson '351 with Kodama's enhancement implemented. Hubner invites combination with other backup techniques: “Regardless of the approach employed, data backup may be performed due to data loss, file corruption, computing system failure or the like. These techniques can be employed **in conjunction with the peer-distributed**, network-controlled data backup and restoration services of platform 103.” APPL-1030, [0013]. Further, Hubner describes that it applies to “data of all types” and is directed to substantially similar user devices interacting with a data management platform over a network that is similar to the cloud storage of Jakobsson '351. APPL-1003, ¶248; APPL-1030, [0014], [0022], [0023], FIG. 1, APPL-1011, 7:2-5. Adding peer-to-peer communications feature for backup/restore would merely have been applying a known technique to a known device (method, or product) 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 Jakobsson '351 device as enhanced by Kodama. APPL-1003, ¶248. Further, POSITA would have had an expectation of success as the teachings of Kodama provide for mitigating compatibility issues between the peer-to-peer exchange by ensuring the peer devices are a same brand. *Id.*

3. Claim 5

5. *The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.*

Claim 1 is rendered obvious by Jakobsson '351 and Kodama and claim 5 is rendered obvious by Jakobsson '351, Kodama and Hubner. APPL-1003, ¶¶249-253. Hubner describes a system that provides for a first device and a second device to be configured to complete a *pairing process*, *see supra* IX.B.3.

Therefore, claim 5 is rendered obvious by Jakobsson '351, Kodama and Hubner.

4. Claim 6

6. *The system of claim 5, wherein the pairing process comprises a comparison of data generated from one or more authentication inputs.*

Claim 6 is obvious over Jakobsson '351, Kodama and Hubner. APPL-1003, ¶¶254-258.

First, Hubner describes its peer-to-peer backup process (a *pairing process*) requires each device register with data management platform 103 that operates the

backup process; it would have been obvious for the registration to be compared in the authentication process as discussed *supra* IX.B.4. APPL-1030, [0016], [0030], FIG. 2, [0031].

To the extent Patent Owner argues the claims require it, implementing a biometric authentication would have been obvious. POSITA would have found it obvious to increase the security of Hubner's pairing process by biometric authentication, a well-known authentication technique. APPL-1003, ¶257.

Thus, claim 6 is obvious over Jakobsson '351, Kodama and Hubner.

5. Claims 24-25

Claim 24 is rendered obvious by Jakobsson '351, Kodama and Hubner for the reasons discussed with respect to claims 5 and 18; claim 25 is rendered obvious by Jakobsson '351, Kodama and Hubner for the reasons discussed with respect to claims 6 and 18. APPL-1003, ¶259.

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.
- 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-

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.

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 the claims it challenges are **not asserted** in the Parallel District Court Proceeding. *See* APPL-1029, 2. Moreover, Apple stipulates that, if the Board institutes this Petition and IPR2024-00333, it will not pursue the grounds raised in either petition in the Parallel District Court Litigation. *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 Challenger, 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 13,935 (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 APPL-1001–APPL-1017, APPL-1019–APPL-1021, APPL-2023–APPL-1038; 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