

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

**DECLARATION OF PATRICK MCDANIEL,
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITION FOR
INTER PARTES REVIEW**

TABLE OF CONTENTS

I.	Introduction.....	7
II.	Qualifications and Professional Experience	10
III.	Level of Ordinary Skill in the Art	14
IV.	Relevant Legal Standards	16
V.	Overview of the '105 Patent.....	20
VI.	Technology Background.....	29
	A. AUTHENTICATION.....	29
	B. CREDENTIALS AND CREDENTIAL MANAGEMENT.....	30
	C. CRYPTOGRAPHY	34
	D. CRYPTOGRAPHY IN WEB TRANSACTIONS.....	35
	E. TRUSTED PLATFORM MODULES	36
VII.	Claim Construction.....	38
VIII.	Claims 1, 2, 4-6, 12, 15, 18, 21, 23-25, 31, and 34 are Unpatentable	39
	A. Ground 1: Claims (1), 2, 4, 12, 15, (18), 21, 23, 31, and 34 are obvious under 35 U.S.C. § 103 over Kesanupalli, Cheng and Kodama.....	41
	1. Summary of Kesanupalli	41
	2. Summary of Cheng.....	43
	3. Summary of Kodama	46
	4. Reasons to Combine Kesanupalli, Cheng and Kodama.....	48
	5. Claim 1	56
	a) [1.0] A system, comprising:	56

b)	[1.1] <i>one or more processors configured to:</i>	57
c)	[1.2] <i>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;</i>	59
d)	[1.3a] <i>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,</i>	64
e)	[1.3b] <i>wherein the credential information comprises a cryptographic key;</i>	72
f)	[1.4] <i>receive authentication input from the user;</i>	74
g)	[1.5] <i>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;</i>	75
h)	[1.6] <i>retrieve at least a portion of the credential information from the at least one record stored on the first device;</i>	78
i)	[1.7] <i>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</i>	80
j)	[1.8] <i>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</i>	84
k)	[1.9] <i>a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.</i>	88
6.	Claim 2	89

7.	Claim 4	90
8.	Claim 12	92
9.	Claim 15	94
10.	Claims 18, 21, 23, 31 and 34.....	97
B.	Ground 2: Claims 5, 6, 24 and 25 are obvious under 35 U.S.C. §103 over Kesanupalli, Cheng, Kodama and Hubner.....	99
1.	<i>Hubner</i>	99
2.	<i>Combination of Kesanupalli, Cheng, Kodama and Hubner</i> .	101
3.	<i>Claim 5</i>	108
4.	<i>Claim 6</i>	114
5.	<i>Claims 24 and 25</i>	117
C.	Ground 3: Claims 1, 2, 4, 12, 15, 18, 21, 23, 31, and 34 are obvious under 35 U.S.C. § 103 over Jakobsson 351 and Kodama.....	118
1.	Jakobsson 351 and Kodama	118
2.	Reasons to Combine Jakobsson 351 and Kodama.....	118
3.	Claim 1	122
a)	[1.0] <i>A system, comprising:</i>	122
b)	[1.1] <i>one or more processors configured to:</i>	122
c)	[1.2] <i>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;</i>	122
d)	[1.3a] <i>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,</i>	123

e)	[1.3b] wherein the credential information comprises a cryptographic key;.....	124
f)	[1.4] receive authentication input from the user;.....	124
g)	[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;	124
h)	[1.6] retrieve at least a portion of the credential information from the at least one record stored on the first device;	125
i)	[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	125
j)	[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	126
k)	[1.9] a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.	129
4.	Claim 2	129
5.	Claim 4	130
6.	Claim 12	131
7.	Claim 15	132
8.	Claims 18, 21, 23, 31, 34.....	133
D.	Ground 4: Claims 5-6 and 24-25 are obvious under 35 U.S.C. §103 over Jakobsson '351, Kodama and Hubner.	135
1.	Hubner	135

2.	Combination of Jakobsson '351, Kodama and Hubner	135
3.	Claim 5	142
	<i>[5.0] The system of claim 1, wherein the first device and the second device are configured to complete a pairing process.....</i>	<i>142</i>
4.	Claim 6	146
5.	Claims 24-25	148
IX.	Conclusion	149

I, Patrick McDaniel, do hereby declare as follows:

I. INTRODUCTION

1. I make this declaration based upon my own personal knowledge and, if called upon to testify, would testify competently to the matters stated herein.

2. I have been asked by Apple Inc. (“Apple”) to provide my expert opinion connection with the *Inter Partes* Review of U.S. Patent No. 11,475,105 (“’105 patent”) concerning whether the ’105 patent is unpatentable over certain prior art. This declaration is a statement of my opinions on issues relating to the patentability of Claims 1, 2, 4-6, 12, 15, 18, 21, 23-25, 31, and 34 (“the Challenged Claims”) of the ’105 patent. As I explain more fully below, it is my opinion that all the Challenged Claims would have been obvious to a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention.

3. I am being compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary expenses associated with my work and testimony in this investigation. My compensation is not contingent on the outcome of this matter or the specifics of my testimony. I have no other financial interest in this proceeding.

4. I have reviewed and considered the following documents in connection with my analysis of the ’105 patent:

a) the ’105 patent, APPL-1001;

- b) the prosecution history of the '105 patent (“’105 File History”),
APPL-1002;
- c) U.S. Patent No. 8,799,666 to Kesanupalli et al. (“Kesanupalli”),
APPL-1006;
- d) U.S. Patent No. 8,099,789 to Challener et al. (“Challener”),
APPL-1007;
- e) U.S. Patent Publication No. 2004/0117636 to Cheng et al.
 (“Cheng”), APPL-1008;
- f) European Patent Application EP 2 079 023 A2 published
15.07.2015 (“Kodama”), APPL-1010;
- g) U.S. Patent Application No. 2012/0150808 to Hubner et al.
 (“Hubner”), APPL-1030; and
- h) U.S. Patent 10,360,351 (“Jakobsson ’351”), APPL-1011.

5. In forming the opinions expressed below, I have considered:

- a) the documents listed above;
- b) the relevant legal standards, including the standard for
obviousness, and any additional authoritative documents as cited in the body of
this declaration; and
- c) my own knowledge and experience based upon my work in the
field of authentication and distributed computing as described below, as well as the

following materials:

APPL-1009	U.S. Patent No. 9,652,629 (“Brown”)
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-1019	Computer Dictionary, Second Edition, entry “data 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-1023	RFC2818, HTTP Over TLS (May 2000)
APPL-1024	https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf
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

6. Unless otherwise noted, all emphasis in any quoted material has been added.

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My Curriculum Vitae (CV) is attached as APPL-1004. This exhibit also includes a list of my publications and the cases in which I have testified at deposition, hearing, or trial within the past four years.

8. I earned a Ph.D. in Computer Science from the Computer Science and Engineering Department at University of Michigan, Ann Arbor in 2001. I earned a Bachelor of Science degree in Computer Science from Ohio University in 1989, and a Master of Science degree, also in Computer Science, from Ball State University in 1991.

9. Since 2022, I have been Tsun-Ming Shih Professor of Computer Sciences in the School of Computer, Data and Information Sciences at the University of Wisconsin-Madison. Prior to my move to Wisconsin, I was the William L. Weiss Professor of Information and Communications Technology in the School of Electrical Engineering and Computer Science at the Pennsylvania State University in University Park, PA. I was also the director of the Institute for Network and Security Research, and founder and co-director of the Systems and Internet Infrastructure Security Laboratory, a research laboratory focused on the study of security in diverse network and computer environments. My research efforts primarily involve computer systems (including authentication), network management and authentication, systems security, and technical public policy.

10. Prior to 2017 I was an Assistant Professor (2004-2007), Associate Professor (2007-2011), Full Professor (2011-2015), and Distinguished Professor (2016-2017) of Computer Science and Engineering and the William L. Weiss Professor of Information and Communications Technology (2017-2022) at the Pennsylvania State University. Since 2004, I have taught courses in the field of computer systems, systems programming, mobile device security, networks, and network and computer security at both the undergraduate and graduate level. I created and maintained several of these courses at Penn State and Wisconsin.

11. From 2003-2009, I was also an Adjunct Professor at the Stern School

of Business at New York University in New York, NY. At the Stern School of Business, I taught courses in computer and network security and online privacy.

12. I am a Fellow of the Association for Computing Machinery (ACM, the leading professional association for computer science), a Fellow Institute for Electrical and Electronics Engineering (IEEE, the leading professional association for engineering), and Fellow of the American Association for the Advancement of Science (AAAS, the leading professional association for science).

13. I am the director of the NSF Frontier Center for Trustworthy Machine Learning (CTML), a research organization exploring security and privacy of machine learning (and AI in general). Funded by the US National Science Foundation, the CTML is led by the University of Wisconsin-Madison and has members from Stanford, the University of California, Berkeley, The University of California-San Diego, and the University of Virginia.

14. From 2013 to 2018 I was the Program Manager (PM) and lead scientist for the Cyber Security Collaborative Research Alliance (CRA). The CRA is led by Penn State University and includes faculty and researchers the Army Research Laboratory, Carnegie Mellon University, Indiana University, the University of California-Davis, and the University of California-Riverside. This initiative is a major research project aimed at developing a new science of cyber-security for military networks, computers, and installations.

15. I regularly advise students on research projections covering aspects of computer systems security. In this role, I regularly serve as an advisor to Ph.D. and master's degree candidates, several of whom have gone on to become professors at various institutions such as North Carolina State University, Purdue University, the University of Toronto, the University of Oregon, the Georgia Institute of Technology and the University of Florida.

16. Before joining Pennsylvania State University as a professor, from 1991 - 1996 I was a software developer and project manager for companies in the networking industry including Applied Innovation, Inc., and Primary Access Corporation. I was also a senior researcher at AT&T Research-Labs. As part of my duties in these industrial positions, I informed, reviewed, and formed corporate policies and practices relating to the security of mobile devices, networks, and software systems.

17. I have published extensively in the field of authentication, mobile security, network and security management, computer systems, authentication, systems security, applied cryptography and network security. In addition to writing several articles for industry journals and conferences, I have authored portions of numerous books related to computer systems (including authentication), applied cryptography and network security. I have served on the editorial boards of several peer-reviewed journals including ACM Transactions on Internet Technology, for

which I was the Editor-in-Chief. I was also an Associate Editor for ACM Transactions on Information and System Security and IEEE Transactions of Software Engineering, two highly regarded journals in the field.

III. LEVEL OF ORDINARY SKILL IN THE ART

18. I understand there are multiple factors relevant to determining the level of ordinary skill in the pertinent art, including (1) the levels of education and experience of persons working in the field at the time of the invention; (2) the sophistication of the technology; (3) the types of problems encountered in the field; and (4) the prior art solutions to those problems.

19. I understand that the '105 patent was filed December 15, 2020 and claims priority as a continuation in part through various applications to provisional applications filed January 17, 2012 and December 9, 2011. As I discuss below (see Section V.), the effective filing date of the claims of the '105 patent is the actual filing date (December 15, 2020) of the continuation-in-part application (U.S. Appl. 17/123,018) that issued as the '105 patent. While the '105 patent claims priority through a chain of earlier filed application, those claims of priority are unsupported due to the absence of disclosure in the documents to which priority is claimed for a “based at least in part on the first device being a same brand as a second device” limitation.

20. Here, a POSITA at the time of the claimed invention 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 biometric authentication techniques, and related firmware and software, or the equivalent, with additional education substituting for experience and vice versa. A person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for a POSITA. For purposes of this Declaration, in general, and unless otherwise noted, my statements and opinions, such as those regarding my experience and the understanding of a POSITA generally (and specifically related to the references I consulted herein), reflect the knowledge that existed in the field as of the actual filing date of the '105 patent (*i.e.*, December 15, 2020), but I have also considered the knowledge that existed as of the earliest possible priority date (*i.e.*, December 9, 2011).

21. Unless otherwise stated, when I provide my analysis below, the relevant knowledge and understanding is consistent with the that of a POSITA just prior to the earliest possible priority date of the '105 patent—December 9, 2011—as well as that at the actual filing date of the '105 patent—December 15, 2020. Unless specifically stated, none of my analysis relies on a greater level of POSITA knowledge or understanding as of the later date.

22. I met the definition of a POSITA in 2011 and 2020. I also had a

greater knowledge and experience than a POSITA. In my work discussed above, including as a professor, I worked with graduate students and others who had the knowledge and experience of a POSITA in 2011 and 2020, and I am able to render opinions from the perspective of a POSITA based on my knowledge and experience.

IV. RELEVANT LEGAL STANDARDS

23. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '105 patent, I am relying on certain basic legal principles that counsel have explained to me. These principles are discussed below.

24. Obviousness: I have been informed that a claimed invention is unpatentable under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. I have also been informed by counsel that the obviousness analysis takes into account factual inquiries including the level of ordinary skill in the art, the scope and content of the prior art, and the differences between the prior art and the claimed subject matter.

25. I have been informed by counsel that the Supreme Court has recognized several rationales for combining references or modifying a reference to

show obviousness of claimed subject matter. Some of these rationales include the following: (a) combining prior art elements according to known methods to yield predictable results; (b) simple substitution of one known element for another to obtain predictable results; (c) use of a known technique to improve a similar device (method, or product) in the same way; (d) applying a known technique to a known device (method, or product) ready for improvement to yield predictable results; (e) choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; and (f) some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

26. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected results of the invention, any long-felt but unsolved need in the art that was satisfied by the alleged invention, the failure of others to make the alleged invention, praise of the alleged invention by those having ordinary skill in the art, and copying of the alleged invention by others in the field. I understand that there must be a nexus—a connection—between any such secondary considerations and the alleged invention.

I also understand that contemporaneous and independent invention by others is a secondary consideration tending to show obviousness.

27. I am not aware of any allegations by the named inventor of the '105 patent or any assignee of the '105 patent that any secondary considerations are relevant to the obviousness analysis of any Challenged Claim of the '105 patent.

28. Priority Date: I understand that, for any given claim of the '105 patent, prior art includes patents and printed publications in the relevant art that predate the effective filing date of that claim. I understand that, subject to the next paragraphs, the “priority date” of a patent is the earlier of: (a) the date on which a patent application that later issues as the patent is actually filed; or (b) the date on which an earlier-filed patent application is filed if the patentee properly claims the benefit of priority to the earlier-filed patent application.

29. I understand that merely claiming the benefit of an earlier-filed application is insufficient. In particular, in order for the earlier priority date to be applicable, the prior application must describe the claimed invention, and must do so in sufficient detail that one skilled in the art can clearly conclude that the inventor had possession of the claimed invention as of the filing date sought. I am told that the priority-date analysis is on a claim-by-claim basis. I understand that in order for a patent claim of a later-filed application to be entitled to the filing date of an earlier-filed patent application, the earlier-filed patent application must meet

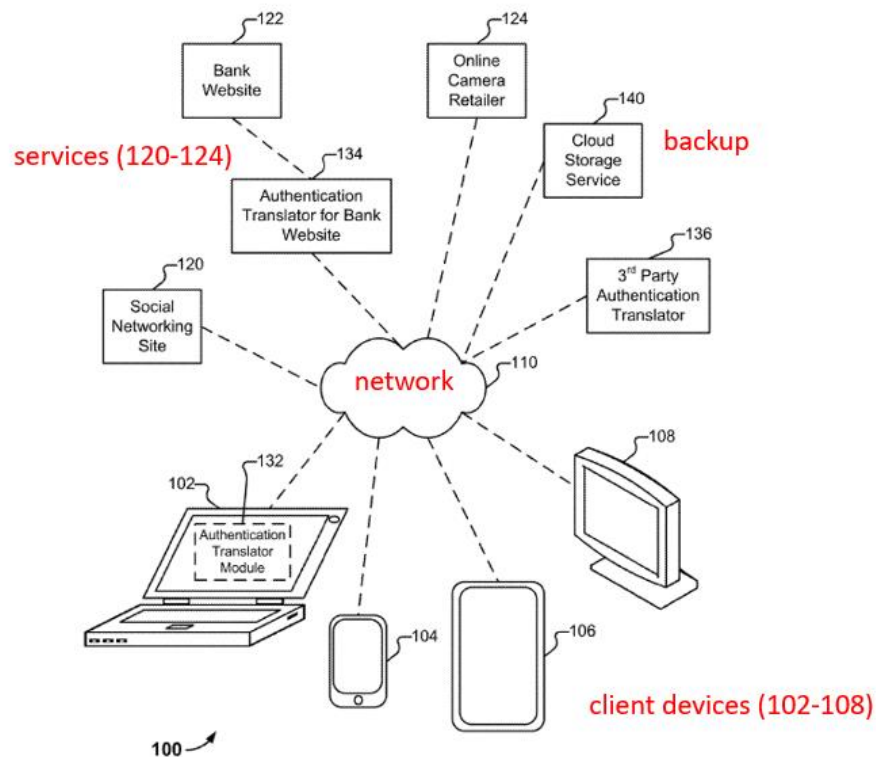
both a written-description and an enablement requirement for that patent claim as of the filing date of the earlier-filed patent application. I also understand that this analysis may be referred to as an analysis of compliance with 35 U.S.C. § 112. I understand that it is not sufficient that the claim would have been obvious from the earlier application, rather the earlier-filed patent application itself must describe the claimed invention.

30. I understand to satisfy the written description requirement the earlier-filed patent application must reasonably convey to those skilled in the art that the inventors had possession of the subject matter of sought to be claimed by the later-filed patent as of the filing date of the earlier-filed patent application. I have been informed that it is disclosures of the earlier-filed patent application that count, and that while the meaning of terms, phrases, or diagrams in the earlier-filed patent application must be interpreted from the vantage point of a POSITA, all of the claimed limitations must be disclosed in the manner later claimed. Further, I understand that this analysis is not a question of whether one skilled in the art *might* be able to construct the later-filed patent application's claimed invention from the teachings of the disclosure or whether that claimed invention is an obvious variant of that which is actually disclosed in the specification of the earlier-filed patent application; rather, I understand that the earlier-filed patent application must itself describe each of the claim limitations expressly or

inherently. I also understand that in order to satisfy the enablement requirement, the earlier application must enable a person of ordinary skill in the art to practice the claimed invention of the later-filed patent application without undue experimentation.

V. OVERVIEW OF THE '105 PATENT

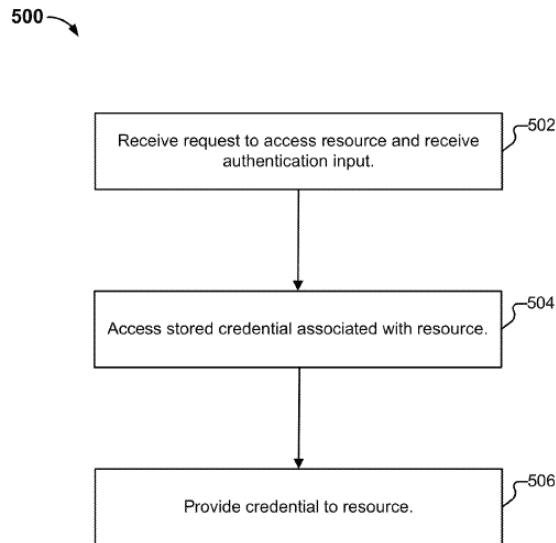
31. The '105 patent is directed to an environment that includes a client device, such as a notebook computer, smartphone, or tablet, which is connected via a network such as the Internet to a service such as a website. ('105 patent) APPL-1001, 2:62-3:14. FIG. 1 the '105 patent illustrates such an environment including client devices (102-108) connected to services (120-124).



(’105 patent) APPL-1001, FIG. 1, annotated

32. The ’105 patent describes authentication techniques to provide user credentials (e.g., a password) from a client device to a service with a goal of avoiding reliance on a user’s input of the credential, which is tedious for the user and leads to poor security practices. (’105 patent) 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.” (’105 patent) APPL-1001, 3:20-26. FIG. 5 of the ’105 patent illustrates a process for

performing this authentication translation. ('105 patent) APPL-1001, 1:66-67.



(’105 patent) APPL-1001, FIG. 5

33. The ’105 patent describes an example of FIG. 5 where a user, Alice, wishes to sign onto a social networking website 120. Alice is prompted by her client device, in this example her laptop, to provide biometric information using an “integrated fingerprint reader on her laptop.” (’105 patent) APPL-1001, 6:50-7:3. Alice provides her biometric information in response to the prompt. *Id.* A translation module such as provided in her laptop compares her provided biometric information with a template stored on the computer. (’105 patent) APPL-1001, 7:3-10. If a match is found, a previously stored credential associated with the resource is provided to the resource. (’105 patent) APPL-1001, 7:11-16. These techniques for authentication translation were well-known by 2011.

34. ’105 Prosecution History: I have reviewed the file history of the ’105

patent, which I understand is attached as APPL-1002. In an office action, the Examiner rejected many of the pending claims as obvious indicating a then pending dependent claim 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, (Office Action dated 01-28-2022) at p. 17. In response, the applicant amended each of its independent claims to include the limitation very similar to that indicated to be allowable. Representative claim 1 as amended is reproduced below:

1. (Currently amended) A system, comprising:
 - one or more processors configured to:
 - 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;
 - 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, wherein the credential information comprises a cryptographic key;
 - receive authentication input from the user;
 - 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;
 - retrieve at least a portion of the credential information from the at least one record stored on the first device;
 - 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
 - based at least in part on the first device being a same brand as a second device,
 - initiate a backup, to ~~[[a]]~~ the second device, of at least a portion of the at least one record;
 - and
 - a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.

APPL-1002, Response dated June 17, 2022, 2. Following the amendment, a notice of allowance issued and did not further discuss the Examiner's reasons for allowance. APPL-1002, Notice of Allowance dated 07/21/2022, 3.

35. However, prior to the '105 patent, it was well-known to, based at least in part on the first device being a same brand as a second device, initiate a backup, to the second device as I discuss in this declaration.

36. Effective filing date of Application that issued as the '105 Patent: I

understand a continuation-in-part (CIP) patent stems from an application that claims priority to a prior application but adds additional subject matter not disclosed in the prior application. And I understand that the '105 Patent issued on a continuation-in-part (CIP) application (US Application 17/123,018, “the '018 Application”) filed December 15, 2020. I am informed by counsel (and note from the front page of the '105 patent (APPL-1001, (63)), the '018 Application claims priority as CIP to U.S. Application 17/027,481 (“the '481 Application”), which in turn claims priority through a chain of five (5) continuation applications originating with US Application 13/706,254 (“the '254 App”), filed December 5, 2012.

37. I have reviewed '018 Application and understand it was originally filed with a dependent claim 16 that contained the language “wherein 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. No written description exists in any prior application to which the '018 Application claims priority—including the '481 Application and '254 Application—that provides support for a backup being performed *in response to a determination* that the first device is *of the same brand* as the second device.

38. Claims 1, 18 and 35 of the '105 patent include the limitation “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, of at least a portion of the at least one record.” I have reviewed each of the applications to which the ’105 patent claims priority (see APPL-1005) and no written description exists in any application to which its ’018 Application claims priority - including the ’481 Application and ’254 Application - for this element. Initiating backup to a second device was based at least in part on the first device being a same brand as a second device was first presented in the ’108 Application filed on December 15, 2020.

39. I note that the ’018 Application discusses concepts related to backup and “brand” at pages 21 ([0073]) and 29 ([0083]), which provide text corresponding to that of the ’105 patent at column 13:28 – 33 and column 19:29 – 35. These passages are reproduced below at the highlighted portions:

In some embodiments, a policy associated with a vault determines whether a vault may be backed up. ... Policies can also be associated with devices, or with all vaults on a device. Such a policy may state that vaults can only be backed up to computational devices of the same brand, or to computational devices that satisfy software requirements associated with the policy, such as having anti-virus software or using an operating system that is the most recent version or the version before that, but not older.

..

There are various ways of securely conveying vaults or vault contents from one computational device to another. ... In addition, the employer of the user may have a policy stating that only devices that are on the employer's approved list of devices may be used, where in various embodiments this approved list includes types or brands of devices, Media Access Control (MAC) address ranges, etc.

I note that these passages are not found any application to which the '018 Application claims priority. Rather, these passages, like the general concept of initiating a backup to a second device based at least in part on the first device being a same brand as the second device, were first presented in the '018 Application filed on December 15, 2020. I note these passages fall under a heading "ADDITIONAL EMBODIMENTS," which I conclude to include additional subject matter, such as the concept of performing backup based on a determination that two devices are of a same brand, introduced by the applicants in filing the '018 Application.

40. After review of each and every application to which the '018 Application claims priority, I conclude that each such application lacks a corresponding disclosure. Moreover, it is my opinion that each such application lacks any written description that a POSITA would understand to establish possession of the claim limitation "based at least in part on the first device being a

same brand as a second device, initiating a backup,” or any concept of performing backup based on a determination that two devices are of a same. For this analysis, I have considered for each such application what a POSITA would understand the application to disclose as of the actual filing date of that application. In my opinion, only the '018 Application itself contains disclosure that a POSITA would understand to establish possession of the claim limitation “based at least in part on the first device being a same brand as a second device, initiating a backup,” or any concept of performing backup based on a determination that two devices are of a same.

41. Thus, to summarize, it is my conclusion that the support for the limitation “based at least in part on the first device being a same brand as a second device, initiating a backup” is provided only with respect to the '018 Application as of its actual filing date of December 15, 2020 and that no such support appears in any of the other applications to which it claims priority, which are listed below and provided in APPL-1005:

Serial Number	Filing Date	Issued Patent No.	Issue Date	Disclosure of initiating backup based at least in part on “brand”
17/123,018	Dec 15, 2020	'105 patent	10/18/2022	Described
17/027,481	Sept 21, 2020	11,514,138	11/29/2022	None
16/773,767	Jan 27, 2020	10,929,512	02/23/2021	None

16,563,715	Sept 6, 2019	10,824,696	11/03/2020	None
16/273,797	Feb 12, 2019	10,521,568	12/31/2019	None
15/042,636	Feb 12, 2016	10,360,351	07/23/2019	None
13/,706,254	Dec 5, 2012	9,294,452	03/22/2016	None
61/587,387	Jan 17, 2012			None
61/569,112	Dec 9, 2011			None

VI. TECHNOLOGY BACKGROUND

42. To provide background for my discussion of the prior art and the element-by-element analysis of the claims that follows, I present an overview of some of the relevant state of art at existing at the time of the alleged invention of the '105 patent. The background below I discuss relevant technologies and techniques. To provide background for my discussion of the prior art and the element-by-element analysis of the claims that follows, I present an overview of some of the relevant state of art at existing at the time of the alleged invention of the '105 patent. The background below I discuss relevant technologies and techniques.

A. AUTHENTICATION

43. Authentication is the process of verifying the identity of a user (or system) ensuring that they are (or it is) who they claim to be. This process is essential to protecting systems and data from misuse by non-authorized entities (*e.g.*, hackers, insiders, etc.). The field of authentication for computer systems was well established by at least the 1970s, and methods and tools for its realization are

well documented and widely standardized.

44. The process of authentication typically involves the presentation of a credential by a party to some system. If the credential is verified to be correct, the presenter is authenticated and allowed to use the system. For example, a user may be asked present a password to gain access to a computer. The computer then checks that the password is correct (*e.g.*, using protected data stored on that computer—sometimes represented as a password file). In this situation, the password is a credential.

45. Well before the earliest possible priority date of December 9, 2011, authentication was a well-established practice for users of computers and information systems.¹ Users of devices and information systems (including websites) interacted with and relied on these authentication systems to establish their identity and ultimately their authorization to access protected information.

B. CREDENTIALS AND CREDENTIAL MANAGEMENT

46. Early authentication methods developed for computerized systems relied upon a password as a credential as described above. These systems

¹ APPL-1012, Patrick McDaniel, *Authentication*, Handbook of Computer Networks, Volume II, Chapter 171, John Wiley and Sons, May, 2007. Eds. Hossein Bidgoli.

prompted users to provide a password credential, which when provided was compared to a list of passwords stored in the system to ensure the user was who they claim to be.

47. Long before the earliest possible priority date of the '105 patent, authentication methods progressed from use of a simple password to provide additional security. Authentication systems, again well before the earliest possible priority date of the '105 patent, were based on one or more of three kinds of credentials: things you know (*e.g.*, passwords), things you have (*e.g.*, a card), or things you are (*e.g.*, fingerprints). *See also*, (Kesanupalli) APPL-1006, 4:31-35. In all three types of authentication factors, the systems rely on assessing presented credentials to compare the presented credential against some stored information for the purposes of validation.

48. The third type of authentication factor (things you are) is referred to as biometric authentication. Biometrics as a field is well-established, with systems that measure biometrics such as fingerprints, irises, and facial recognition being widely used since the 1990s, and some biometric authentication techniques dating to the 1970s and before. Biometric systems typically use sensors such as touchscreens/surfaces, camera, or other means to measure some aspect of the user's body. Fingerprint readers identify ridges on a finger; cameras capture images that are used to estimate facial dimensions; iris scanners record unique

contours and patterns in the user's eye. Prior to the earliest possible priority date, biometric systems on user devices were widely used and indeed advertised as a more convenient and secure way to protect a user's electronic devices. For example, touchpads serving as biometric sensors were integrated into hardware and sold on commodity systems.²

49. When using biometrics for authentication, a set of biometric features—often called a template—such as features corresponding to a user's fingerprint are stored for example as a data file. This stored template is compared to a later biometric input (*e.g.*, a reading from a fingerprint sensor) often using a fuzzy matching algorithm. If the later biometric input is sufficiently similar to the template, the identity of the user may be deemed authentic.

50. A security architecture that commonly leveraged biometrics for authentication prior to the earliest possible priority date of the '105 patent was “single sign-on” or SSO.³ In SSO, users initially login to a client device such as their computer through an authentication service relying upon password, hardware

² 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>

³ See, *e.g.*, APPL-1014; U.S. Patent Publication 2008/0059804 to Shah et al. [0003]-[0044].

token or biometric input such as discussed above. After having logged in through the single authentication input, the user could access multiple applications or systems. That is, after a successful login, the SSO would retrieve a credential from storage on the client device or create one (*e.g.*, an authentication token) associated with the applications or systems. This credential was then used to gain access to the application or system rather than requiring the user to perform a separate authentication to each. Here, the user only logs in once, which provides access to credentials to all other supported services. Some of the earliest SSO solutions appeared in the late 1990s.⁴

51. As even the earliest authentication systems compared a user's input with a stored credentials (*e.g.*, password lists, biometric templates), the need to protect these credentials from unauthorized access was immediately clear. Authentication applications such as SSO increased the need to manage security of stored credentials. One typical way to protect of a user's authentication data and credentials was by using cryptography. Here, authentication-related data was (and is) almost always stored in persistent storage (*e.g.*, on hard drives or in databases) in encrypted format—and thus protected from compromised systems.

⁴ See, *e.g.*, APPL-1015, <https://gost.isi.edu/publications/kerberos-neuman-tso.html>

C. CRYPTOGRAPHY

52. Cryptography is the science of secret writing, which is an incredibly deep and widely studied technology. In computers, it is used to secure data and communication. Specifically—and among other things—cryptography can be used for a goal of protecting confidentiality and/or integrity (protecting against corruption) of data.

53. Perhaps the most widely used cryptographic algorithm is encryption. In its simplistic form, in some implementations, an encryption function E that takes some data (plaintext P) and a cryptographic key K_e produces new data (called ciphertext C) that hides the original data, i.e., $E(K_e, P) = C$. A decryption function D associated with the given encryption function E takes the ciphertext and a decryption key K_d and produces the original plaintext, i.e., $D(K_d, C) = P$. The important part is that the plaintext P cannot feasibly be recovered from the ciphertext C without K_d ⁵, and therefore the encryption protects the underlying plaintext P from access by users who do not possess the decryption key K_d .

⁵ Note that in many cases, K_e and K_d are the same. Such algorithms are called symmetric key algorithms in this case. Prior to 2000s, an alternative to symmetric-key cryptography was developed that use a public-key cryptography, which uses a pair of keys: public (K^+) and private (K^-). In public-key cryptography, data encoded with either key, can be decoded using the other key.

54. Encryption for protection of data such as a passwords relied on secure message authentication codes (MACs), which are functions that take a sequence of bytes as input and output a new sequence of bytes. One type of MAC is a hash-based MAC or HMAC. In HMAC, a key is additionally used as input to the MAC, so that the output of the HMAC depends both on the input bytes as well as the key value. Common (and indeed standardized) HMACs in use at the time of patent included the use of hash functions such as SHA-1 and SHA-2. Cryptographic systems of MAC and HMACs were in use in at least the early 1990s, many years prior to the earliest possible priority date of the '105 patent. Regardless of what algorithm is used or what its function it performs all uses of cryptographic algorithms (e.g., encryption, decryption, hashing, HMACing) are cryptographic operations.

D. CRYPTOGRAPHY IN WEB TRANSACTIONS

55. Authentication and use of encryption techniques for web transactions was widely used prior to the earliest possible priority date.

56. HTTP cookies were developed at least in the 1990s. An HTTP cookie is a small block of data created by a webserver while a user is browsing a website. The HTTP protocol allows for the transfer of a cookie from the server to the client device. Web browsers store cookies on the client device (*e.g.*, the user's device), and the HTTP protocol allows for a webserver to request that the client send a

cookie previously created by the server. When a user sends login information to a site (say, by providing a username and credential such as a password), the server can respond by setting a cookie on the client. The cookie encodes the fact that the user has logged in. Subsequently, the server can request the client's cookie(s), and when it receives the cookie, it can check whether its encoding indicates that the user has logged in. Thus, the website can continue operations without repeatedly requiring the user to provide username and password.

57. Authentication may also be performed using public-key encryption. In the 1990s, Netscape Communications developed Secure Socket Layer (SSL). SSL, which evolved into transport layer security (TLS), is the basis for secure data transfer on the Web. By 2011, much of the electronic commerce conducted was done using the SSL/TLS and public-key cryptography.

E. TRUSTED PLATFORM MODULES

58. In the early 2000s with expansion of the computing industry, there was a need to allow personal devices to be more resistant to unauthorized access to its data.

59. By 2006, new computing systems with Trusted Platform Module (TPM) chips were being sold.⁶ A Trusted Platform Module (TPM) is a specialized

⁶ APPL-1016, <https://www.iso.org/standard/50970.html>

microprocessor or hardware coprocessor that is designed to provide security-related functions through restricted interfaces. The typical role of a TPM in a computing system is to securely store and generate cryptographic keys, as well as to perform security related operations such as key and credential management, authentication, facilitating securing storage, encryption, decryption, and digital signatures.

60. The TPM works in concert with less secure elements of the computing system (such as a general-purpose CPU or exposed interfaces or resources) and with applications running on such elements to perform security related operations for overall system. Most of the security of the TPM is derived from the isolation of security-related data and computations from the general-purpose CPU and from other less secure elements of the host machine. Because the security-related data and computations are not directly exposed to a (potentially compromised) operating system and/or applications that instead interact (via the TPM) with secure storage maintained and secure operations performed by the TPM itself, the system is able to security notwithstanding the risk of programs running on less secure elements of the computing system.

61. TPM provides physical and application programming interfaces (APIs) that restrict access to security-related operations such as key and credential management, secure storage, encryption, decryption and digital signatures. More

specifically, TPM APIs are called by privileged programs, the operating system, firmware to access the security sensitive data and functions implemented within the TPM processor.⁷ The APIs allow the caller to create code that implements critical security functions for the systems and applications, *e.g.*, access securely stored cryptographic keys, encrypt sensitive data (called sealing), or obtain cryptographically strong random data. Because of the sensitivity of the functions and data in the TPM, access to these APIs is tightly controlled by the operating system (typically through permissions). By the earliest possible priority date of the '105 patent, TPMs were widely used in the computer industry. By 2008, there were over 100 million PCs shipped with TPMs.⁸ Such devices were widely used in commercial applications including securing storage, authenticating users and software, and supporting secure network applications.

VII. CLAIM CONSTRUCTION

62. It is my understanding that in order to properly evaluate the '105 patent, the terms of the claims must first be interpreted. It is my understanding that for the purposes of this *inter partes* review, the claims are to be construed under

⁷ APPL-1017, https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf

⁸ APPL-1024, <https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf>

the so-called *Phillips* standard, under which claim terms are given their ordinary and customary meaning as would have been understood by one of ordinary skill in the art in light of the specification and prosecution history, unless the inventor has set forth a special meaning for a term. For the purposes of this declaration, it is my opinion that the claim terms should be given their plain and ordinary meaning.

VIII. CLAIMS 1, 2, 4-6, 12, 15, 18, 21, 23-25, 31, AND 34 ARE UNPATENTABLE

63. I have been asked to provide my opinion as to whether Claims 1, 2, 4-6, 12, 15, 18, 21, 23-25, 31, and 34 of the '105 patent ("Challenged Claims") would have been obvious in view of the prior art. The discussion below provides a detailed analysis of how the prior art references identified below teach the limitations of the Challenged Claims of the '105 patent.

64. As part of my analysis, I have considered the scope and content of the prior art and any differences between the alleged invention and the prior art. Below, I describe in detail the scope and content of the prior art, as well as any differences between the alleged invention and the prior art, on an element-by-element basis for each Challenged Claims of the '105 patent.

65. As described in detail below, the alleged invention of the Challenged Claims would have been obvious in view of the teachings of the identified prior art references as well as the knowledge of a POSITA. I apply the prior art as follows:

Grounds	Claim(s)	Basis
#1	(1), 2, 4, 12, 15, (18), 21, 23, 31, and 34	§103 over Kesanupalli, Cheng and Kodama
#2	5-6, 24-25	§103 over Kesanupalli, Cheng, Kodama and Hubner
#3	(1), 2, 4, 12, 15, (18), 21, 23, 31, and 34	§103 over Jakobsson '351 and Kodama
#4	5, 6, 24, 25	§103 over Jakobsson '351, Kodama and Hubner

66. With respect to Grounds #1 and #2, I understand from Counsel that the '105 patent claims priority to Provisional Application No. 61/587,387 filed on Jan. 17, 2012 and Provisional Application No. 61/569,112 filed on Dec. 9, 2011. I have used the earliest possible priority date – Dec. 9, 2011 – for my analysis of this declaration with respect to Grounds #1 and #2. I understand from Counsel that each of Kesanupalli, Cheng, and Hubner qualify as prior art with respect to this earliest possible priority date. My analysis equally applies to the proper priority date – Dec. 15, 2020 – for my analysis of this declaration with respect to Grounds #1 and #2.

67. With respect to Grounds #3-#4, I determined that the first instance of support for the claims is found on the filing of the Serial No. 17/123,108 on December 15, 2020 as discussed above. I have used this priority date – Dec. 15, 2020 – for my analysis of this declaration with respect to Grounds #3-#4. I

understand from Counsel that Jakobsson 351, Kodama, and Hubner qualify as prior art with respect to this priority date of Dec. 15, 2020.

A. Ground 1: Claims (1), 2, 4, 12, 15, (18), 21, 23, 31, and 34 are obvious under 35 U.S.C. § 103 over Kesanupalli, Cheng and Kodama.

1. Summary of Kesanupalli

68. U.S. Patent No. 8,799,666 to Kesanupalli *et al.* (“Kesanupalli”) issued from an application filed on March 24, 2010 and is entitled “Secure User Authentication Using Biometric Information.” (Kesanupalli) APPL-1006, (22), (54).

69. Kesanupalli is directed to a secure authentication system that uses biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” (Kesanupalli) APPL-1006, 1:1-2:59-62. For example, 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. (Kesanupalli) APPL-1006, FIGS. 8, 9.

70. 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

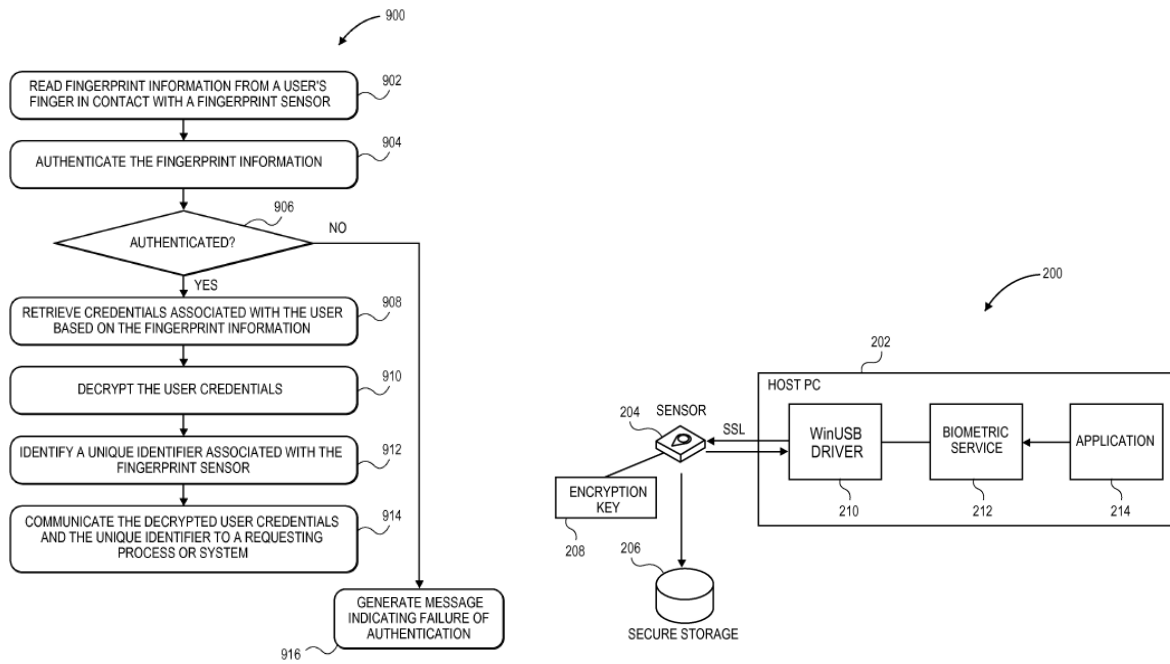
be distinguished from fingerprints associated with other users.” (Kesanupalli) APPL-1006, 3:33-41. The user (or system) also “provides user credentials, such as a password, cryptographic key ... or the like,” and the systems and methods described in Kesanupalli “bind the user’s fingerprint template with the user credentials.” (Kesanupalli) APPL-1006, 3:15-18, 3:41-46. To further protect user credentials, “[t]he fingerprint template and user credentials are then stored in a secure storage of the user’s device.” (Kesanupalli) APPL-1006, 3:46-47, *see also*, (Kesanupalli) APPL-1006, 5:61-6:49.

71. 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.” (Kesanupalli) APPL-1006, 3:52-59. “[T]he user credentials released after finding a matching fingerprint template may include an OTP (One Time Password) token, RSA signature and the like.” (Kesanupalli) APPL-1006, 3:62-4:1, 3:41-44, FIG. 12.

72. FIG. 9 of Kesanupalli (shown below) illustrates these steps of authenticating a user in the context of an embodiment in which user credentials are cryptographically secured in storage. FIG. 2 (also shown below) 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.

(Kesanupalli) APPL-1006, 6:26-49, 9:10-24.



(Kesanupalli) APPL-1006, FIGS. 9 and 2

73. In an authentication process, the biometric 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.

(Kesanupalli) APPL-1006, 6:31-45. The released credentials are then

communicated to the external resource by an application 214 of the Host PC 202.

(Kesanupalli) APPL-1006, FIG. 2, 5:9-58, 6:11-31.

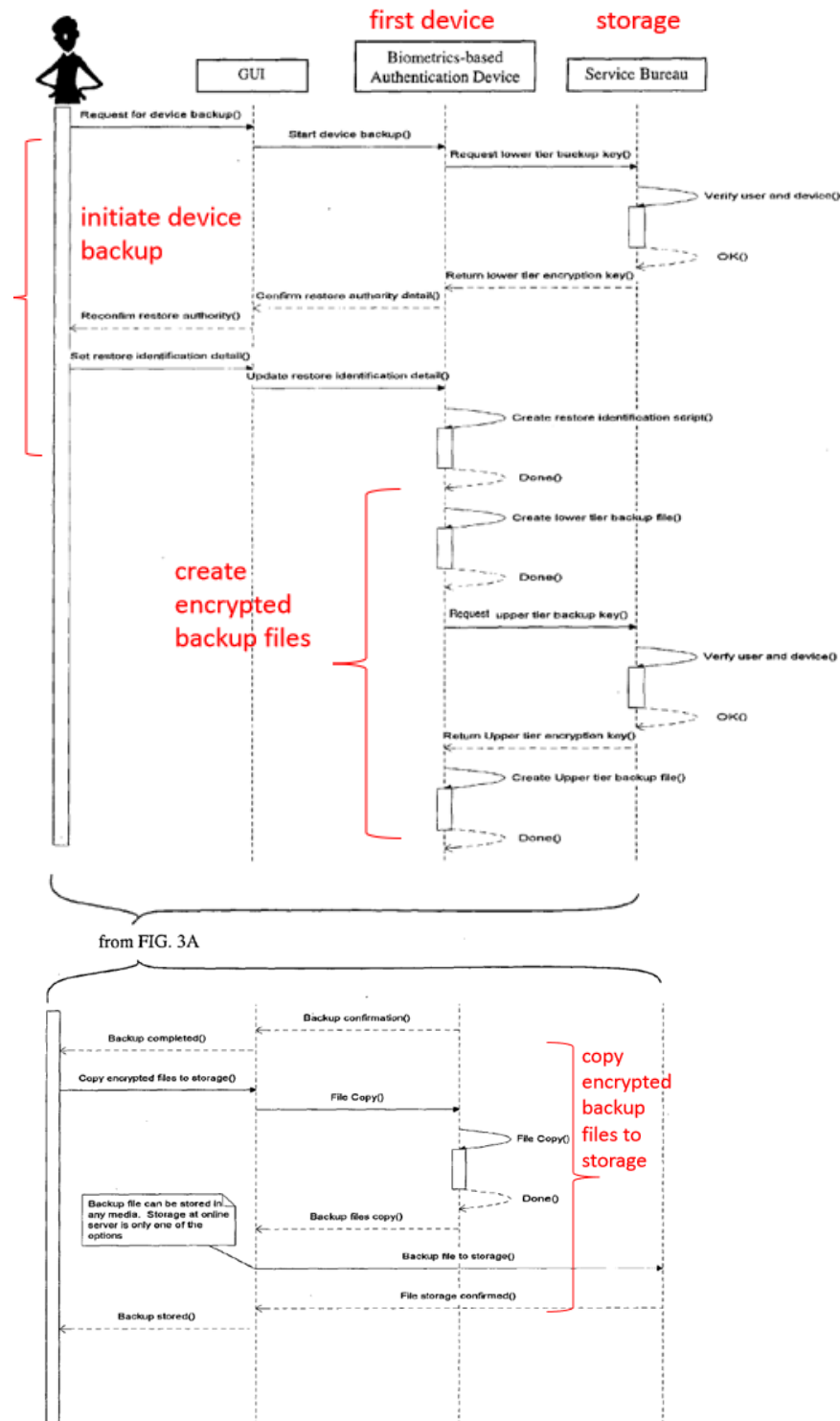
2. Summary of Cheng

74. Cheng is entitled "System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information" and was filed Sep. 24,

2003 and published Jun 17, 2004. (Cheng) APPL-1008, (54), (220), (43).

75. Cheng recognizes “[w]ith the rapid growth of computers, electronics, communications, networks, and the Internet, access control in general and network security in particular have become increasingly important for obvious reasons.” (Cheng) APPL-1008, [0003]. “Data, property interests, personal identity as well as personal safety could be at risk if security is breached” and to satisfy security needs, authentication systems, methods, and devices are needed to “certify the validity of an identity, account, object, and so on.” *Id.* 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.” (Cheng) APPL-1008, [0004], [0006].

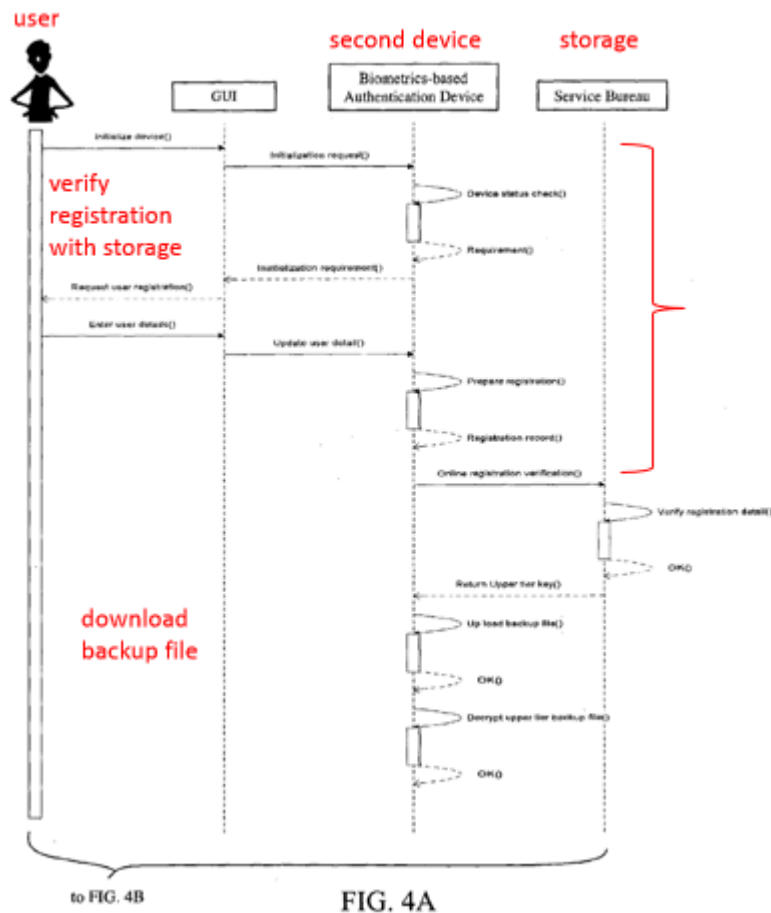
76. Cheng performs a secure backup of this data to avoid costs of creating the data on new device from scratch should a first device containing the data be lost or stolen. *See* (Cheng) APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng’s FIGS. 3A-3B where a backup of data of a first user’s device is performed through secure communication between a user service bureau (storage) and the device. (Cheng) APPL-1008, [0029]-[0030]. Cheng’s backup process includes a two-tier encryption of the backed-up data. (Cheng) APPL-1008, [0007] – [0008], [0031]-[0039], FIGS. 3A, 3B.



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

77. Cheng describes a use case of a user's first device, having been

backed-up to a user service (a storage service), becoming unavailable. A secure connection is provided between the user service and a second device to retrieve the backed-up data downloaded to the second device. See (Cheng) APPL-1008, [0044]–[0050], FIGS. 4A–4C.



(Cheng) APPL-1008, FIG. 4A, annotated

3. Summary of Kodama

78. Kodama is also directed to backing up data in an electronic device.

(Kodama) APPL-1010, (57), [0040], [0041]. While Kodama centers around

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

79. Like Cheng, Kodama teaches registering a first device with a backup service. (Kodama) APPL-1010, [0101]. Kodama provides additional details as to this registration process including that the process includes providing “device information including the manufacturer name, model name.” *Id.* Kodama continues to describe a backup process including sending data of the registered first device to the backup service. *See* (Kodama) APPL-1010, [0106] – [0107].

80. In an example, Kodama explains using the backup service the data is then restored onto another device (e.g., a “new” device) and to start the restoration process, “device information including the manufacturer name, model name and product serial number” of the second device is sent to the backup service system. (Kodama) APPL-1010, [0135] – [0136]. The backup service system then verifies the device information – the manufacturer name and model number – of the second device before permitting the backup of data to the second device. (Kodama) APPL-1010, [0137], [0138], [0143]-[0144].

4. Reasons to Combine Kesanupalli, Cheng and Kodama

81. A POSITA would have been motivated to apply Cheng's teachings of backing up data from storage of an electronic device, such as the device used in Kesanupalli that stores user's biometric information and credentials for user authentication to resources such as websites, to a second device. Kesanupalli's stored biometric information and credentials are a user's personal data, and applying Cheng's back up teachings would produce the obvious, beneficial, and predictable results of reducing the need to recreate the user's personal data when using a new device, such as on a device replacing a lost or stolen device. Kodama provides additional details as to implementing a backup of data from an electronic data from a first device to a second device, including ensuring the devices are a same brand, which provides the obvious, beneficial and predictable result of mitigating complexity, compatibility and security issues.

82. I now explain further the mitigating complexity, compatibility and security issues by initiating the backup to the second device based at least in part on the first device being a same brand as the second device. First, implementing this backup procedure would have been recognized as allowing the developer of the system to rely on brand specific implementations that ensure that all devices in a product line can leverage the backup service (compatibility) with minimal interfaces tailored to the homogeneous interface design (complexity). Matching

the brand results in a small, closed source (not public) design and codebase that uses credentials and cryptographic keys that need only be created and known to the manufacturer—and thus provides strong security. A POSITA would have recognized these benefits long before the '105 patent.

83. Kesanupalli, Cheng, Kodama and the '105 patent are all in the same field of endeavor such as security arrangements and procedures for protecting data in computer systems. *See, e.g.*, (Kesanupalli) APPL-1006, 32:30-38 (“[S]ystems and methods described herein relate to biometric authentication of users. ... biometric information provides an additional level of security when used in systems and procedures related to authentication of a user.”), 2:48-50 (“client device, such as a computer, cellular phone, and so forth”); (Cheng) APPL-1008, [0003], [0004] (“Data, property interests, personal identity as well as personal safety could be at risk if security is breached. To satisfy different security needs, various authentication systems, methods, and devices exist today and new ones are continually being developed.”) ('105 patent) APPL-1001, 1:43-52 (“Providing credentials to a service, whether via a mobile or other device, is often a tedious experience for a user. ... users will often engage in practices ... which render their credentials less secure against attacks. Accordingly, improvements in authentication techniques would be desirable.”), FIG. 1 (showing client devices of notebook computer 102, smartphone 104, tablet 106); (Kodama) APPL-1010, (57)

(“The risk of a third party referring to or using back-up data with authorization upon restoring such backup data in an HDD recorder is mitigated”), [0040] (“The backup target application is not limited to an HDD recorder, and...can be applied to any electronic appliance such as a mobile phone, a PDA or a PC...”), [0041].

84. Moreover, as evidenced on the front page of Kesanupalli, the '105 patent, and Kodama the international classification (IPC), U.S. classifications (CPC) and/or the field of search classification consulted by the Office during examination for each patent include the same subclass, namely CPC/IPC G06F 21 (security arrangements for protecting computers, components thereof, programs or data against unauthorized activity). *See* ('105 patent) APPL-1001, (51), (52); (Kesanupalli) APPL-1006, (51) (58); (Kodama) APPL-1010, (51); *see also* www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (subclass definitions); www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (CPC to IPC concordance). Cheng does not include a search classification; however, a POSITA would recognize that it also is suitable for consideration as being directed to such technology and falls under the same field of endeavor. APPL-1008, [0007] (“Enabling technologies include biometrics, authentication, cryptography, and encryption/ decryption.”) Cheng’s disclosure is directly applicable to security arrangements for protecting computers, components thereof, programs or data against unauthorized activity, as Cheng provides security

procedures having a goal of protecting data (e.g., by encryption) in the backup process. Cheng also similarly directed to protection of a user's authentication data. (Cheng) APPL-1008, [0004], [0007]; (Kesanupalli) APPL-1006, FIG. 2, Abstract; ('105 Patent) APPL-1001, 3:39-56.

85. Second, a 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. A POSITA would have understood – in the absence of Cheng's functions - the stored personal data (biometric information and credentials) would need to be created and registered from scratch should the device be lost or stolen. Cheng recognizes this same problem:

In the event of loss, damage, or destruction of the device, the user's authentication information, electronic identity and any data associated therewith would be lost forever. Indeed, to prevent or at least to minimize the possibility of compromising the secrecy of the electronic identity and the authentication information, when a portable authentication device is reported loss or stolen, the general practice is to first deactivate or erase completely from the authentication system or secure network the electronic identity and authentication information associated with the lost/stolen authentication device and then create and

register new ones from scratch.

(Cheng) APPL-1008, [0006].

86. Such a problem of inconvenience would have also been reasonably pertinent to the inventor of the challenged patent. *See* ('105 patent) APPL-1001, 8:55-58 (noting “[s]ince user data can be frequently backed up to the cloud storage, and recovered from this using the new device registration process, inconvenience to the user will be minimized” [when wiping a device])). A POSITA have been motivated to address this problem by combining Cheng with Kesanupalli to address known risks of theft and loss of devices and recovery of data.

87. In particular, a POSITA would readily recognize a personal electronic device can be lost, damaged, or otherwise require replacement. *See* (Kesanupalli) APPL-1006, 10:13-18; (Cheng) APPL-1008, [0006]. And when introducing replacement devices, it is desirable to provide have access to the personal data without having to create the data from scratch. (Cheng) APPL-1008, [0006]-[0007]. Moreover, a POSITA would have recognized a desire in the market of electronic devices to be capable of being backed up long before the '105 patent.⁹

⁹ *See, e.g.*, APPL-1020

<https://www.popularmechanics.com/technology/gadgets/how-to/a6819/how-to-restore-your-data-after-a-hard-drive-crash/>

Cheng provides a benefit of the desired backup of personal data to provide access 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. (Cheng) APPL-1008, [0007] – [0009]. This is data that is the same as data stored in Kesanupalli’s device. (Kesanupalli) APPL-1006, 3:32-51.

88. Cheng also recognizes that it was a known practice in the industry to implement procedures that, on the loss or damage of a user’s device, to implement a wiping procedure. Cheng recognizes this same problem:

In the event of loss, damage, or destruction of the device, the user’s authentication information, electronic identity and any data associated therewith would be lost forever. Indeed, to prevent or at least to minimize the possibility of compromising the secrecy of the electronic identity and the authentication information, when a portable authentication device is reported loss or stolen, the general practice is to first deactivate or erase completely from the authentication system or secure network the electronic identity and authentication information associated with the lost/stolen authentication device and then create and register new ones from scratch.

(Cheng) APPL-1008, [0006]. These wiping procedures, such as discussed in U.S. Patent No. 9,652,629 to Brown et al. (APPL-1009) illustrate the need to provide

backup systems to reduce the need to recreate the data. And Cheng continues to introduce a solution of backup of the data to a remote entity, from which the data can be sent to a second device in the event of a wiping of a user's first device. (Cheng) APPL-1008, [0007].

89. Faced with the device of Kesanupalli having the backup technique of Cheng, a POSITA would have had reason to employ Kodama's technique of controlling backup processes such that the device of the data source, and the device targeted to receive the data from the backup, are compatible. 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." (Kodama) APPL-1010, [0157]. See also, (Kodama) APPL-1010, [0158]. A POSITA would recognize benefits of transfer of data between like brands, including format and product proprietary information of data, are the same. As highlighted above, developing brand specific backup solutions for a device can reduce complexity, ensure compatibility among devices in a product line, and be more secure. Ensuring a matching brand would also be recognized by a POSITA to ensure the second device has sufficient compatibility with respect to security protections, at least as sufficient as the first device, for receipt and storage of personal data without introducing risk of potential threats. Further, a manufacturer of a device including an authentication system implements a proprietary system

that frequently includes different features, perform slightly different template matching, support different biometric sensors (e.g., fingerprint sensors), and store different kinds of credentials. Such features act as market differentiators and are used in advertising to entice customers (i.e., users or system manufacturers) to purchase these devices over competitor offerings. Differences in features and algorithms would also necessitate that the fingerprint/credential database be tailored to these custom systems by containing a unique combination of data fields and other structures.

90. A POSITA would have had reasonable expectations of success in adding backup feature such as taught by Cheng as enhanced by Kodama in a biometric authentication system such as taught by Kesanupalli, as Cheng and Kodama are similarly directed to handling of personal information including biometric authentication information in a secure manner. Adding a backup feature would merely have been applying a known technique to a known device (method, or product) that ready for improvement to yield predictable results. Indeed, the backup feature is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices. And enhancement of the backup feature according to Kodama is implemented by a small addition of one or more fields to that routine software executed on generic processing components.

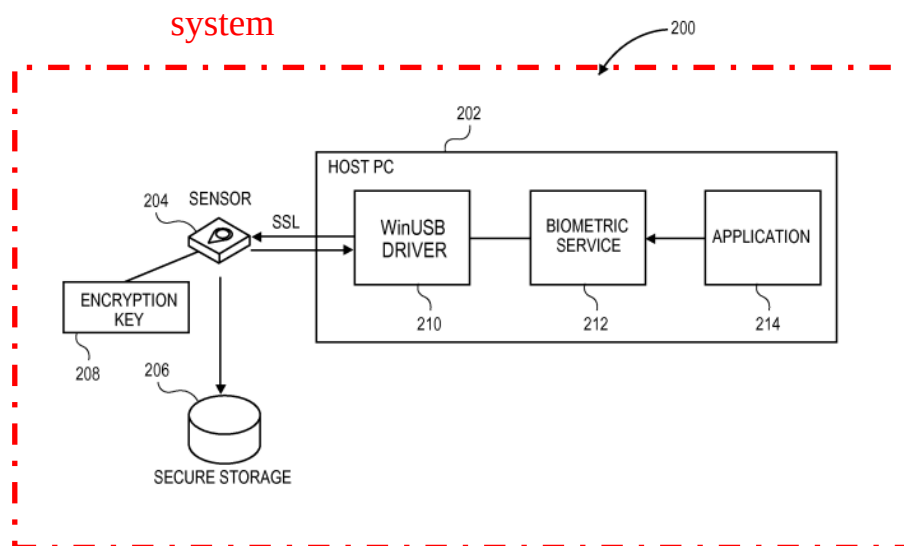
5. Claim 1

a) [1.0] A system, comprising:

91. Kesanupalli discloses *a system*.

92. As illustrated above, Kesanupalli describes in its FIG. 2 a system “capable of performing biometric user enrollment and authentication.”

(Kesanupalli) APPL-1006, 2:1-2. *See also*, (Kesanupalli) APPL-1006, Abstract, FIGS. 11-12.



(Kesanupalli) APPL-1006, FIG. 2, annotated

In Kesanupalli’s system 200, the sensor 204, including its secure storage 206, provides authentication translation and communicates with Host PC 202, which provides communication with external webservers including the communication of the user credential to website. *See* (Kesanupalli) APPL-1006, Abstract, 2:54-3:3,

4:3-11, 4:36-50, 6:11-49, FIG. 12.

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

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

94. Kesanupalli discloses *one or more processors configured to perform the actions of Claim 1 as described in elements [1.2]-[1.9].*

95. Kesanupalli teaches *one or more processors* that are configured to perform the actions of Claim 1 as recited in the following elements. Kesanupalli describes what a POSITA would readily recognize, its described functions of authentication translation and communication with external resources are performed by *one or more processors*:

The invention may also involve a number of functions to be performed by a computer processor, such as a microprocessor. The microprocessor may be a specialized or dedicated microprocessor that is configured to perform particular tasks according to the invention, by executing machine-readable software code that defines the particular tasks embodied by the invention. The microprocessor may also be configured to operate and communicate with other devices such as direct memory access modules, memory storage devices, Internet related hardware, and other devices that relate to the transmission of data in accordance with the invention.

(Kesanupalli) APPL-1006, 9:58 – 10:1.

96. As indicated in the citation above, Kesanupalli also suggests specialized and generalized processors perform its biometric authentication techniques, and a POSITA would understand Kesanupalli to describe implementations in which its biometric authentication techniques are provided using specialized processor executing the authentication functions (those functions of sensor 204 such as authentication or matching) and general processor executing the functions of communicating with an external resource (those of HOST PC 202) together provide *one or more processors*. See (Kesanupalli) APPL-1006, 5:62-6:31 including applications “executing” on the PC 202 and the “match on chip” functionality of sensor 204:

In a particular implementation, biometric sensor 204 includes a “match on chip” functionality that releases a user's credentials only upon a successful fingerprint swipe or other biometric reading. User credentials and other information may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism.

In certain embodiments, the validity biometric service is implemented as a service application running in a local system account.

(Kesanupalli) APPL-1006, 6:40-49. Again, the circuitry providing the processing power for executing the functions of the sensor 204 and the circuitry providing the

processing power for executing the functions of the PC 202 provide *one or more processors*.

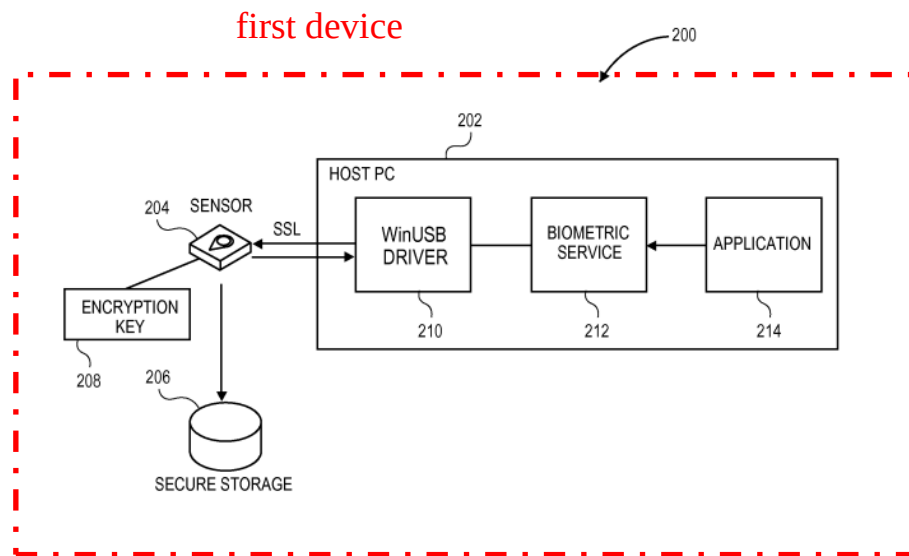
97. Thus, Kesanupalli discloses *one or more processors*.

c) [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;*

98. Kesanupalli discloses *receiv[ing], 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*.

99. First, a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute the *one or more processors* as discussed above. Kesanupalli and, in combination, Cheng and Kodama disclose the functionality, *i.e.*, the processing, that the *one or more processors* is configured to perform and that functionality is described with reference elements [1.2] – [1.8].

100. Turning to element [1.2], Kesanupalli describes a *first device*.

**APPL-1006, FIG. 2, annotated**

101. Biometric sensor 204, its secure storage 206, and Host PC 202 (including web browser application and biometric services 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.

102. Kesanupalli's embodiment illustrated in FIG. 2—and likewise embodiments described relative to FIGS. 1 and 6—constitute such a device, generally defined. *See, e.g.*, APPL-1001, 2:43-45, 3:9-14. Nonetheless, to the extent that Patent Owner some more integrally formed meaning for the term, a POSITA would also understand Kesanupalli to disclose integrally formed realizations of *a device*. Kesanupalli describes the PC 202 and the sensor 204 (including the secure storage 206) are formed as a *device*: “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.” (Kesanupalli) APPL-1006, 2:48-50. *See also*, (Kesanupalli) APPL-1006, 3:46-51 (“In one embodiment the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.”)

103. Kesanupalli describes *receiv[ing]*, at this first device, *a request to access a resource external to the first device*. In particular, Kesanupalli describes *receiv[ing]*, at this first device and in particular at Host PC 202 of the first device, a request (e.g., from user of PC 202) to access a resource (e.g., website) external to the first device. Kesanupalli describes receiving at the first device a request from a user to access a resource (a website) with which the user has already enrolled.

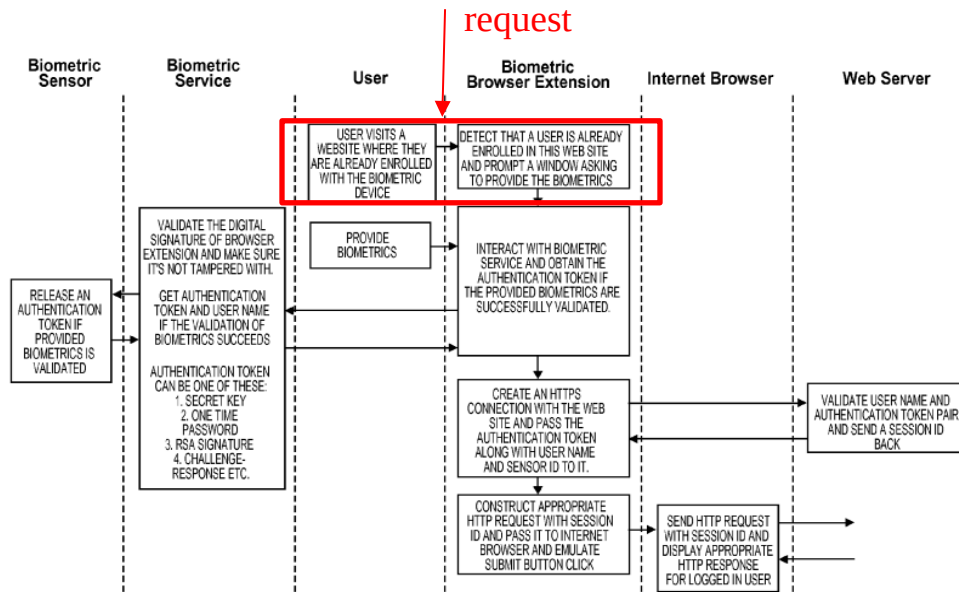
The systems and methods described herein are useful in performing Web site authentication. In example embodiments, a Web site that supports the authentication procedures discussed herein includes an HTML (Hyper Text Markup Language) tag that identifies a Web browser plug-in (also referred to as a “biometric plug-in”) that is installed on the user's computing device. This HTML tag indicates to the browser that the Web site supports biometric authentication. ...

When a user accesses the Web site, the Web browser plug-in is activated

and detects that a biometric sensor is installed in the user's computing device. The Web site suggests that the user enroll with their biometric sensor to provide a more secure user authentication. ...

After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits to the same Web site cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication (e.g., using the biometric device).

(Kesanupalli) APPL-1006, 4:36-5:14, *see also*, (Kesanupalli) APPL-1006, 2:54-3:3, FIGS. 10, 11. FIG. 12 illustrates actions for authenticating a user, including actions performed by a “user,” those actions performed by the user’s device—(e.g., by circuitry of the sensor and applications on the Host PC (e.g., biometric service, browser extension, browser applications), and those by the external resource’s web server. (Kesanupalli) APPL-1006 2:22-24, 9:52-57.



(Kesanupalli) APPL-1006, FIG. 12, annotated

104. In the device of FIG. 2, the request to access the resource is received at the PC 202 (e.g., application 212).

In a particular embodiment, application [] is an Internet browser application executing on host PC [] and communicating with various web servers via the Internet. Application [] includes a browser extension or browser plug-in that communicates with biometric service [].

(Kesanupalli) APPL-1006, 6:11-15, *see also*, (Kesanupalli) APPL-1006,6:28-31.

105. The website visited by the user is *a resource external to the first device* as is it provided on a webserver external to the first device. (Kesanupalli) APPL-1006, 6:11-25, FIG. 12. The website visited by the user is also *a resource*

associated with a user as it is not only a resource that the user has visited, but a resource with which the user has previously enrolled. *See, e.g.,* (Kesanupalli) APPL-1006, FIGS. 7, 11, 3:32-51.

106. Thus, Kesanupalli discloses this element.

d) [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,*

107. Kesanupalli discloses *access[ing] 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.*

108. First, as discussed above, Kesanupalli describes its functions are performed by one or more processors, which includes the functionality described with reference to this element. Generally, Kesanupalli describes its one or more processors perform this element as the sensor 204 accesses a record stored in secure storage 206 – where the record includes both the user’s credentials (e.g., cryptographic key) associated with the external resource (website) to which the user has requested access and the user’s biometric template, which is bound with the user’s credentials, as discussed below. First, Kesanupalli describes a user’s enrollment process in an external resource such as a website where the user’s credential and biometric template are stored in secure storage:

Initially, a user enrolls with the biometric user authentication system by binding their user credentials with the user's biometric template (a “fingerprint template” in specific implementations). The biometric template contains information related to the user's biometric characteristics (also referred to as “biometric information”) obtained from a biometric sensor that scans or reads the user's biometric characteristics, such as a fingerprint. ...

During an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template.... After creating a fingerprint template, the user (or a web server or other system) provides user credentials, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein bind the user's fingerprint template with the user credentials. The fingerprint template and user credentials are then stored in a secure storage device.

In one embodiment the secure storage device is contained within the fingerprint sensor hardware. In other embodiments, the secure storage device is contained in a device that utilizes the fingerprint sensor.

(Kesanupalli) APPL-1006, 3:32-51.

109. 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.”)

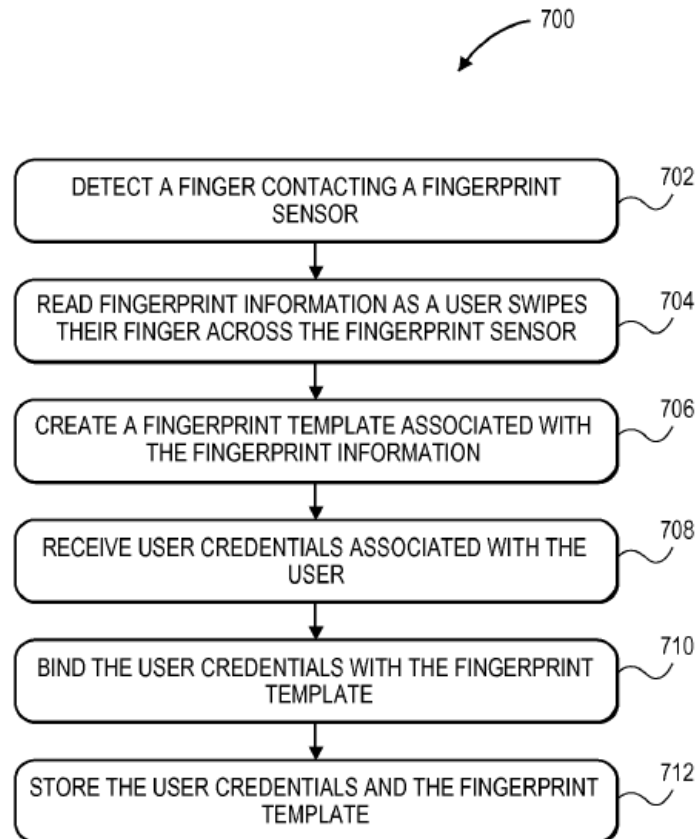


FIG. 7

110. As shown above, Kesanupalli describes a user’s credential bound a biometric template, that is *stored on the first device* in a secure storage. The biometric template is *authentication information associated with the user* as it contains information related to the user’s biometric characteristics. (Kesanupalli) APPL-1006, 2:30-38, 3:14-31. Kesanupalli’s user credential is *credential*

information associated with the external resource (e.g., website) to which the user has requested access. (Kesanupalli) APPL-1006, 4:36-5:43.

The described systems and methods communicate user credentials to a specific address, location, or other recipient identifier. Thus, even if an imposter can gain access to the user credentials, the system will send those user credentials to a predetermined address or location, thereby preventing the imposter from attempting to have the user credentials sent to an alternate address or location. The address or location information is stored within the user credentials and is established as part of the enrollment process.

(Kesanupalli) APPL-1006, 4:3-11.

In particular implementations, the user performs the enrollment process for each Web site the user accesses that supports biometric authentication. Additionally, different user credentials are associated with each Web site with which the user enrolls. Thus, if the user enrolls with five different Web sites that support biometric authentication, the biometric sensor in the user's computing device stores five separate sets of user credentials, each of which is associated with one of the five different Web sites. Additionally, if different users access the same Web site, separate user credentials and separate biometric templates

are maintained for each user.

(Kesanupalli) APPL-1006, 5:33-43. *See also*, (Kesanupalli) APPL-1006, 8:47-53.

111. As Kesanupalli teaches “bind[ing]” the user credentials and the biometric template together and storing them in a storage, they provide a *record*. The record is stored in secure storage 206, part of the first device. (Kesanupalli) APPL-1006, 6:42-49 (“...User credentials and other information may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism...”), FIG. 2, 6:45-49, FIG. 7, 8:40-46, 8:65-9:3, FIG. 11, FIG. 12.

112. It is well known (and indeed taught in first year computer science courses), that computer systems and programs organize related data into records. Considered as the basis for nearly all software design, a record provides a basic data structure that contains different data types or fields grouped together under a single structure, *e.g.*, a block of memory, a compound data type in a program, part of a file in storage, or a row of a table in a database. This grouping allows for the representation of in a structured and organized manner and simplifies the program code and prevents bugs. A POSITA would understand Kesanupalli’s biometric template and user credential to be associated data that is stored and referenced together (in the secure storage), and thus would be represented as a record. A record can be defined as “a data structure that is a collection of fields (or elements).” (Computer Dictionary) APPL-1019. The template and user credential

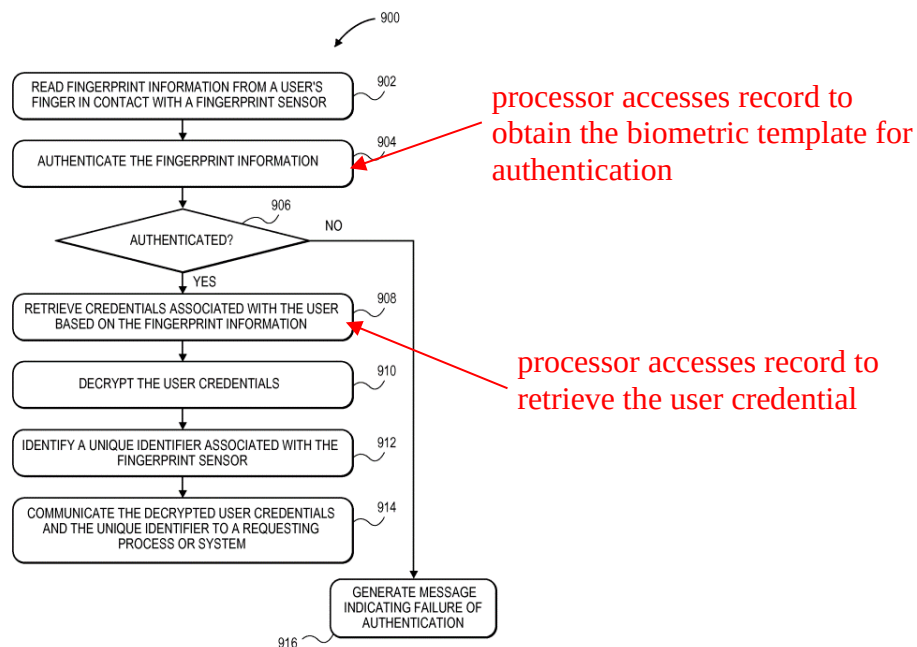
provide a collection of elements together.

113. After enrollment including the creation and storage of the record, subsequent visits by the user to the external resource initiate an authentication translation procedure. (Kesanupalli) APPL-1006, 5:9-14 (“After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits cause...the Web site prompts the user to perform user authentication.”) This authentication process includes the processor(s) *access[ing]* the record in storage to perform the authentication using the biometric template, and *access[ing]* the record in storage to release the credential to the requesting resource. *See also*, (Kesanupalli) APPL-1006, FIGS. 8, 9, 3:51-4:1, 8:54-9:24, FIG. 12 describing the authentication process. FIG. 9 of Kesanupalli is illustrative of the procedure for authenticating a user after she has enrolled in a Web site and illustrates the one or more processors accessing the record:

FIG. 9 is a flow diagram depicting another embodiment of a procedure 900 for authenticating a user of a biometric authentication system. Initially, procedure 900 reads fingerprint information from a user's finger in contact with a fingerprint sensor (902). The procedure then authenticates the fingerprint information (block 904). If the fingerprint information is not authenticated, a message is generated indicating an authentication failure (block 906). If the fingerprint information is

authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (block 910) and identifies a unique identifier associated with the fingerprint sensor (block 912). The decrypted credentials and the unique identifier are communicated to a requesting process or system (block 914).

(Kesanupalli) APPL-1006, 9:10-24. *See also*, (Kesanupalli) APPL-1006 8:54-56.



Kesanupalli, FIG. 9, annotated

114. Referring to the implementation of FIG. 2, Kesanupalli teaches the *one or more processor* on the device and in particular the processor circuitry executing the functions of sensor 204 accesses the biometric template of the record stored in the secure storage 206 in order to authenticate the user through matching

a biometric input with the biometric template of the stored record:

FIG. 2 shows another example system 200 capable of performing biometric user enrollment and authentication via a biometric sensor 204. System 200 includes a host PC 202, a WinUSB driver 210, a biometric service 212 and an application 214 similar to the components discussed above with respect to FIG. 1. In the example of FIG. 2, the biometric sensor decrypts the user credentials only after a successful biometric reading, such as a fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor). For example, in a successful fingerprint swipe, the swiped fingerprint information matches a fingerprint template associated with the fingerprint sensor. In a particular embodiment, the validity enterprise sensor has a unique 256 bit encryption key 208 and a unique identifier (e.g., serial number). The biometric sensor 204 creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique. In a particular implementation, biometric sensor 204 includes a “match on chip” functionality that releases a user's credentials only upon a successful fingerprint swipe or other biometric reading. User credentials and other information may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism.

(Kesanupalli) APPL-1006, 6:31-49.

115. If authenticated, the one or more processors including the circuitry executing the functions of sensor 204 accesses the record as it retrieves the user credentials associated with the requested external resource and communicates the user credentials to the PC 202, which in turn (through processor executing application 212) communicates the credentials “to the Web site to complete the user authentication process.” (Kesanupalli) APPL-1006, 5:22-24. *See also*, FIG. 12. Thus, one or more processors *access* the biometric template of the record for performing this comparison; and also *access* the user credentials of the record stored to release the user credentials upon determining a match in biometrics. *See also*, (Kesanupalli) APPL-1006, 3:52-4:12, 5:17-32, 8:40-53, 9:4-9, 9:17-24, FIG. 12.

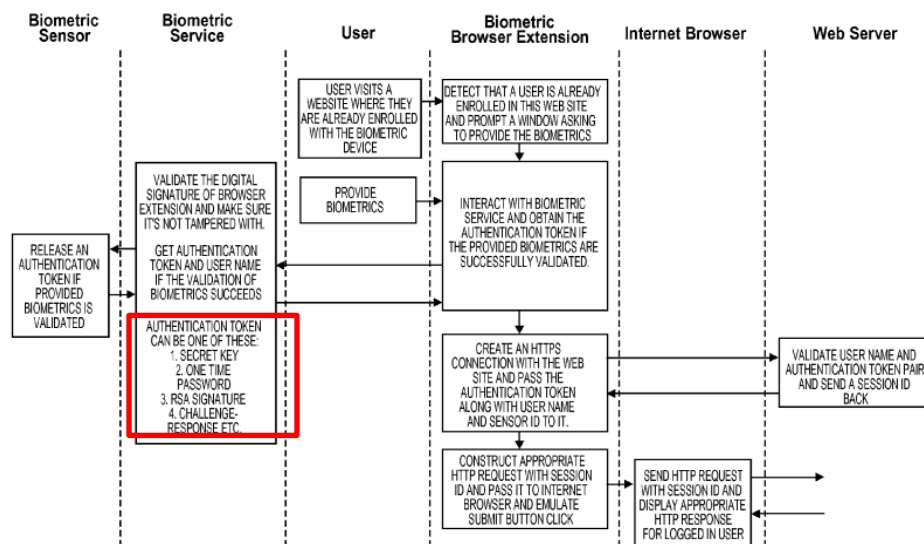
116. Thus, Kesanupalli discloses this element.

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

117. Kesanupalli discloses *the credential information comprises a cryptographic key.*

118. As discussed above in [1.3a], Kesanupalli describes credential information, which it describes as user credentials. Kesanupalli describes one type of user credential is a *cryptographic key*: “The user credentials may be a “password, cryptographic key, random seed, and the like.” (Kesanupalli) APPL-

1006, 3:32-51, *see also*, (Kesanupalli) APPL-1006, APPL-1006, 6:31-36 (“a fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor”), 9:10-24 (“FIG. 9 is a flow diagram depicting another embodiment of a procedure 900 for authenticating a user of a biometric authentication system. Initially, procedure 900 reads fingerprint information from a user's finger in contact with a fingerprint sensor (902).” 8:54-9:3 (“The authentication procedure reads fingerprint information from a user's finger in contact with a fingerprint sensor (block 802).”), FIG. 12 illustrating the user “provide[s] biometrics.” Kesanupalli also describes other types of authentication input from the user. (Kesanupalli) APPL-1006, 2:30-38. Kesanupalli at FIG. 12:



(Kesanupalli) APPL-1006, FIG. 12, annotated

119. Thus, Kesanupalli discloses this element.

f) [1.4] *receive authentication input from the user;*

120. Kesanupalli discloses *receiv[ing] authentication input from the user.*

121. Kesanupalli describes one or more processors *receive an authentication input* (e.g., biometric input such as a fingerprint) *from the user.* In one example, Kesanupalli describes the sensor (204) receives an authentication input of a fingerprint. (Kesanupalli) APPL-1006, 6:31-36 (“a fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor”).

FIG. 9 is a flow diagram depicting another embodiment of a procedure 900 for authenticating a user of a biometric authentication system.

Initially, procedure 900 reads fingerprint information from a user's finger in contact with a fingerprint sensor (902).

(Kesanupalli) APPL-1006, 9:10-24, FIG. 9. *See also*, (Kesanupalli) APPL-1006, FIG. 8, 8:54-9:3 (“The authentication procedure reads fingerprint information from a user's finger in contact with a fingerprint sensor (block 802).”), FIG. 2, 6:31-37, FIG. 12 illustrating the user “provide[s] biometrics.” Kesanupalli also describes other types of authentication input from the user:

The systems and methods described herein relate to biometric authentication of users. ‘Biometrics’ and ‘biometric information’ refers to measurable biological characteristics of a user, such as a fingerprint, facial characteristics, eye characteristics, voice characteristics (also

referred to as a ‘voiceprint’) and the like. As discussed herein, biometric information provides an additional level of security when used in systems and procedures related to authentication of a user.

(Kesanupalli) APPL-1006, 2:30-38.

122. Thus, Kesanupalli discloses this element.

g) [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;*

123. Kesanupalli discloses *determin[ing] 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.*

124. Kesanupalli describes its one or more processors (e.g., processor executing the functions of sensor 204) *determine that the authentication input from the user (e.g., fingerprint from sensor 204) matches the authentication information associated with the user (e.g., fingerprint template) included in the at least one record (e.g., bound template and credential) stored on the first device (e.g., in secure storage 206).* Kesanupalli provides:

During an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor. The process then determines whether the user's fingerprint information matches a fingerprint template associated with the

fingerprint sensor. If the user's fingerprint information matches a fingerprint template, the user's credentials are released to the user and/or a service or process requesting the user verification. Thus, the user credentials are not released from the secure storage device until a matching fingerprint template is confirmed.

(Kesanupalli) APPL-1006, 3:32-51.

125. Kesanupalli describes this process with respect to the authentication procedure of FIG. 9:

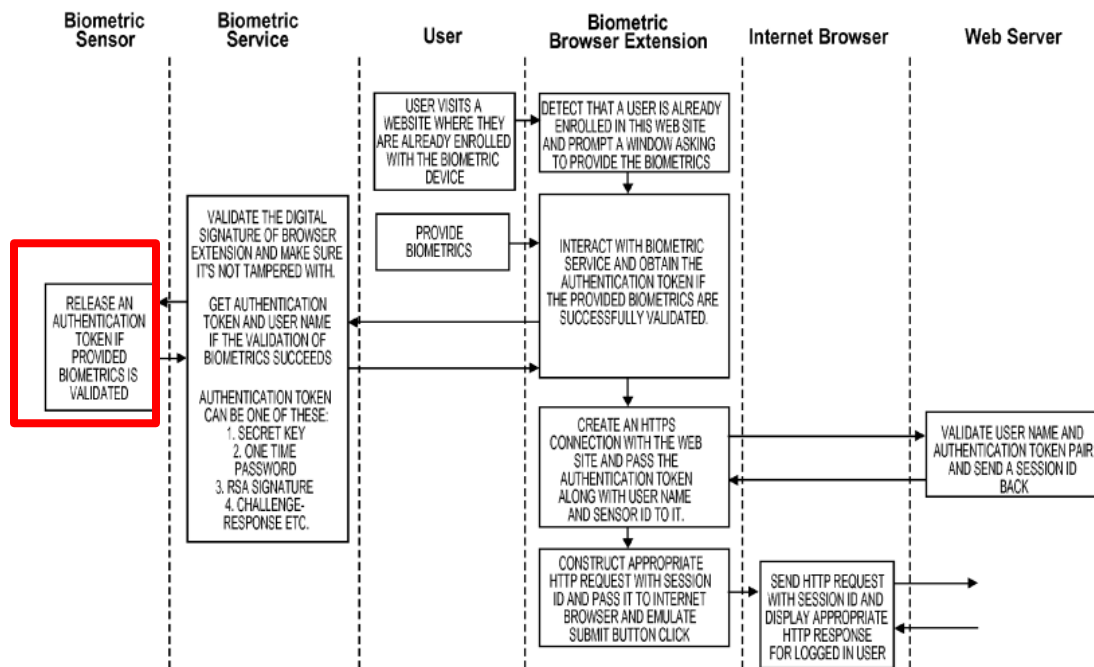
The procedure then authenticates the fingerprint information (block 904). ... If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (910) ...

(Kesanupalli) APPL-1006, 9:14-20. Kesanupalli uses term “authenticat[ing]” input (e.g., user’s fingerprint information), just like “validat[ing]” input, to refer to matching the fingerprint to the template. With respect to the device of FIG. 2, Kesanupalli describes that the processor performing the functions of the sensor 204 executes the matching:

In the example of FIG. 2, the biometric sensor decrypts the user credentials only after a successful biometric reading, such as a

fingerprint swipe or fingerprint scan (using a placement style fingerprint sensor). For example, in a successful fingerprint swipe, the swiped fingerprint information matches a fingerprint template associated with the fingerprint sensor. In a particular embodiment, the validity enterprise sensor has a unique 256 bit encryption key 208 and a unique identifier (e.g., serial number). The biometric sensor 204 creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique. In a particular implementation, biometric sensor 204 includes a “match on chip” functionality that releases a user's credentials only upon a successful fingerprint swipe or other biometric reading. User credentials and other information may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism.

(Kesanupalli) APPL-1006, 6:31-49, FIG. 2. *See also*, (Kesanupalli) APPL-1006, 3:52-4:2, 5:9-24, 8:59-9:9, FIG. 12.



(Kesanupalli) APPL-1006, FIG. 12, annotated

126. Thus, Kesanupalli discloses this element.

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

127. First, as discussed above, Kesanupalli to describes its functions are performed by one or more processors, which includes the functionality is described with reference to this element. As discussed above, Kesanupalli's sensor 204 retrieves the user credential from the secure storage of the device.

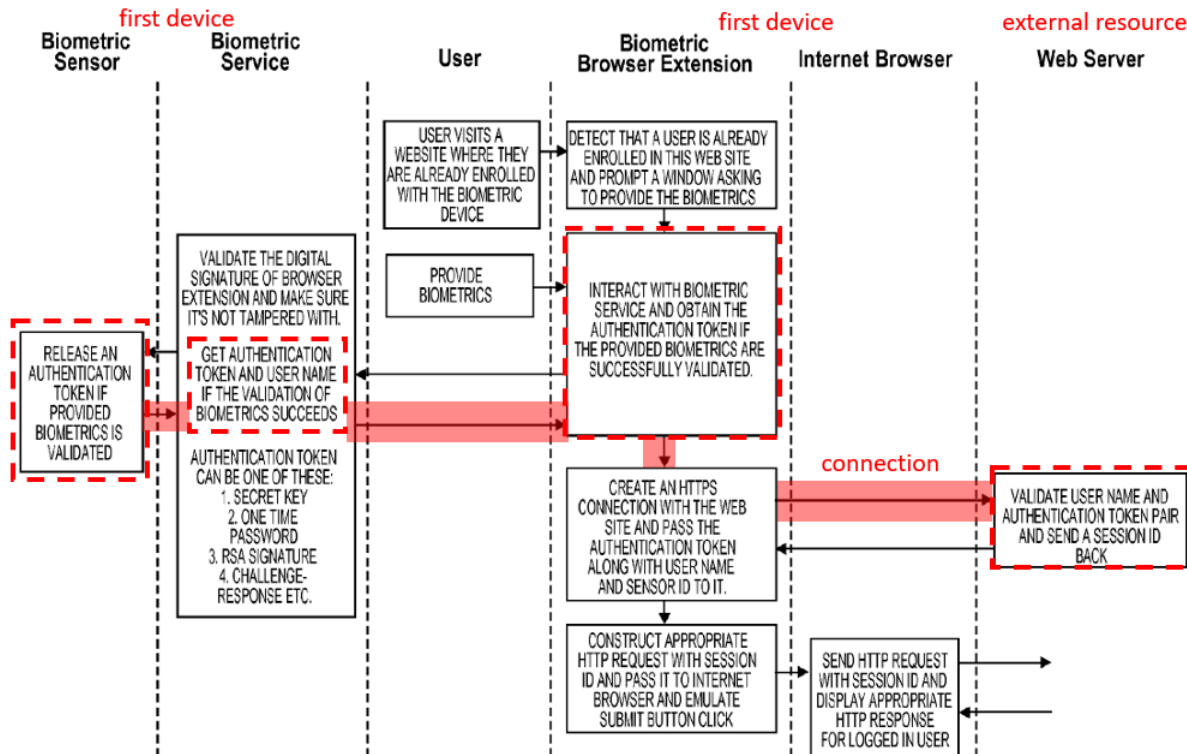
128. In particular, as discussed above in element [1.3a], the *record* (template and credential) is stored in the secure storage 206 of the first device. The credential is retrieved from the record in storage as Kesanupalli describes transferring the credential from the storage to a requesting resource as discussed in

[1.5]. In particular, the credential is retrieved from the record in storage as Kesanupalli describes with respect to the authentication procedure of FIG. 9:

The procedure then authenticates the fingerprint information (block 904). ... If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (910) ...

(Kesanupalli) APPL-1006, 9:14-20.

129. In the context of the system of FIG. 2, the one or more processors (in particular, that of sensor 204) retrieves the credential from record in the storage 206 to provide the credential to the PC 202, which in turn sends the credential to the requesting service. *See also*, (Kesanupalli) APPL-1006, FIG. 2, 3:52-4:11, 5:17-32, 6:42-45, 8:59-9:24. FIG. 12 illustrates actions for authenticating a user, including actions performed by a “user,” those actions performed by the user’s device—(e.g., by circuitry of the sensor and applications on the Host PC (e.g., biometric service, browser extension, browser applications), and those by the external resource’s web server. FIG. 12 is annotated to highlight the path of the credential illustrative of the procedure:



APPL-1006, FIG. 12, annotated

130. Thus, Kesanupalli discloses this element.

i) [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*

131. Kesanupalli discloses element [1.7].

132. First, as discussed above, Kesanupalli to describes its functions are performed by one or more processors, which includes the functionality is described with reference to this element.

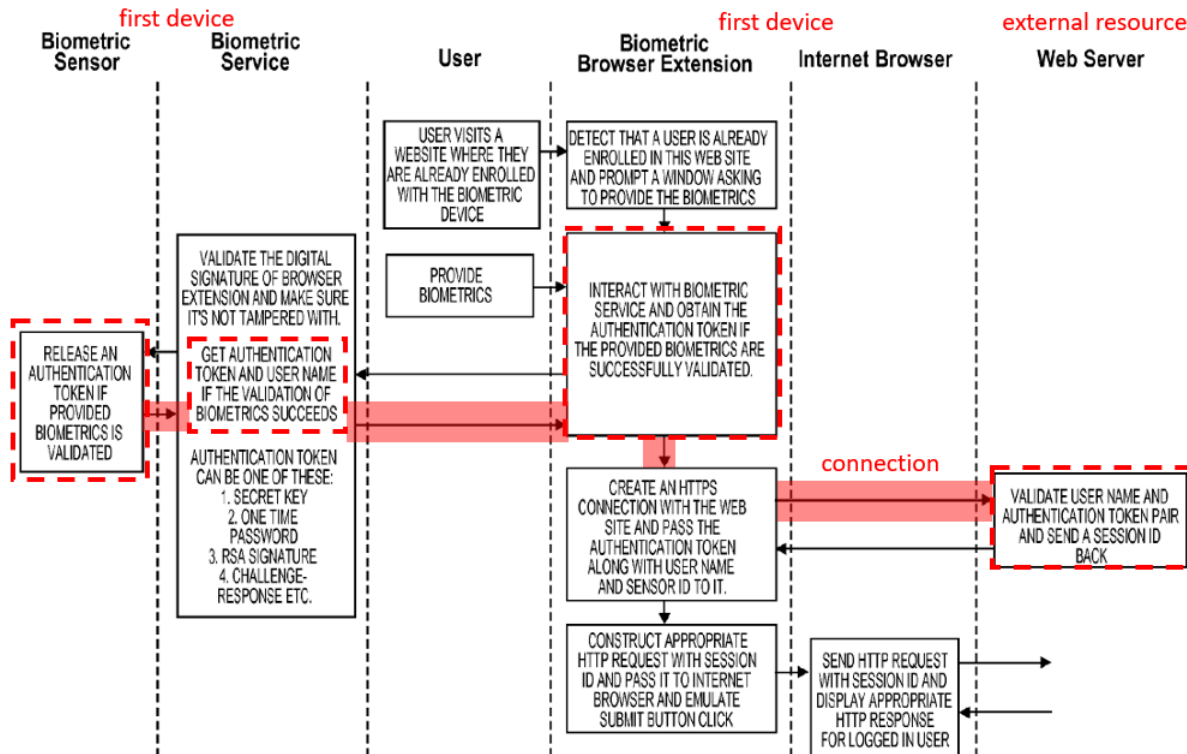
133. In Kesanupalli's device, the one or more processors *facilitate access*

of the user to the external resource (e.g., the website) at least in part by transmitting, on behalf of the user, from the first device (e.g., from storage 206), output (e.g., user credential) based at least in part on the at least portion of the credential information retrieved from the at least one record.

134. Kesanupalli describes its one or more processors (executing the functions of sensor 204 and PC 202) *transmitting*, from the device, *output* (the user credential) to the external resource (website):

... If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (block 910) and identifies a unique identifier associated with the fingerprint sensor (block 912). The decrypted credentials and the unique identifier are communicated to a requesting process or system (block 914).

(Kesanupalli) APPL-1006, 9:10-24. *See also*, APPL-1006, 9:4-9. In the device of FIG. 2, the user credential (e.g., cryptographic key) is retrieved from the secure storage 206 of the sensor 204 and provided to application 214 of PC 202 for communication to the external resource. (Kesanupalli) APPL-1006, 6:11-49. FIG. 12 is annotated to highlight the path of the credential (here referred to as an authentication token) illustrative of the procedure:



(Kesanupalli) APPL-1006, FIG. 12, annotated

See also, (Kesanupalli) APPL-1006, FIG. 2, 3:52-4:11, 5:17-32, 6:42-45, 8:59-9:24 discussing the transmitting of the user credentials and communication with the external resource.

135. When Kesanupalli transmits the user credential to the requesting website as discussed above, it does so on *behalf of the user* as the credential is the user's credential, which is transmitted in response to the user's request to access the website. The user credential (also referred to as an authentication token in Kesanupalli) is *output based at least in part on the at least portion of the credential information* as the output is the credential itself – e.g., the cryptographic key.

136. The *user of the first device is granted access to the external resource*

(website) *based at least in part on the output (user credential) transmitted from the first device on behalf of the user* because the credential is used to log in the user to the external resource. See (Kesanupalli) APPL-1006, FIG. 12 (“logged in user”). It is understood that when Kesanupalli communicates the credentials “to the Web site to complete the user authentication process,” the user is granted access to the website. See (Kesanupalli) APPL-1006, 5:22-24. This is the purpose of Kesanupalli’s authentication and the purpose of the credential.

137. Both Kesanupalli and the ’105 patent describe their communication of credentials to website in terms of SSL (now TLS) or HTTPS protocols. (’105 patent) APPL-1001, 5:38-45 (“If a matching entry is found, the associated...username[] and site credential are extracted from the vault....[n]ext, [1] a secure connection is established between Alice’s computer and the service provider, and [2] Alice is authenticated.... [M]utual SSL can be used.”), (Kesanupalli) APPL-1006, FIG. 12 (“...get authentication token and user name if the validation of biometrics succeeds[, then]...[1] create an HTTPS connection with the website and [2] pass the authentication token along with the user name...to it.” HTTPS, also known as HTTP over SSL or HTTP over TLS, is described in RFC2818. (RFC2818, HTTP Over TLS) APPL-1023, 2 (summarizing TLS connection initiation and HTTP requests over the initiated TLS connection). Thus, Kesanupalli and the ’105 patent describe communication of a decrypted

credential to the website via an established connection in like manners.

138. Thus, Kesanupalli discloses this element.

j) [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*

139. Kesanupalli in view of the teachings of Cheng and Kodama renders obvious *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.*

140. As discussed above, Kesanupalli to describes its functions are performed by one or more processors, which includes the functionality is described with reference to this element. Kesanupalli's one or more processors is operable and suitable to performing instructions to accomplish the functions of Kesanupalli, and also those backup functions of Cheng and Kodama as discussed below. *See also, (Cheng) APPL-1008, [0022] recognizing "[o]nboard microprocessor and communication means [] handle communication...and other processing needs such as establishing a secure connection with a remote service bureau, requesting and returning encryption/decryption keys, creating and copying lower tier and upper tier backup files, and terminating the connection" and (Kodama) APPL-1010, [0037] ("Each PC is equipped with...a processing unit (CPU) for processing data stored in the memory").*

141. First, it would have been obvious to *initiate a backup to [a] second device of a least a portion of the at least one record* in the system of Kesanupalli in light of the teachings of Cheng. As discussed in the reasons to combine above, Cheng teaches that it was a known and desired practice to backup data of a client device such as those of Kesanupalli.

142. In particular, Cheng teaches initiating a *backup* of data of a first device to a second device such as a replacement client device. For example, avoiding recreation of the data which inconveniences a user is a desired feature. Cheng's backup procedure involves registering a first device with a storage location, such as a user service bureau. A "backup file(s)" of the device data is generated and provided from the first device to the user service bureau. *See* (Cheng) APPL-1008, Abstract, [0002], [0007]-[0008], [0023] – [0030], FIGS. 3A and 3B. Cheng describes exemplary types of data for backed up includes user authentication information, such as a key and biometric data, which is the same type of data included in Kesanupalli's record (user credential and biometric template) as discussed above. *See* (Cheng) APPL-1008, [0007], [0008], [0030], FIGS. 3A, 3B.

143. Cheng continues to describe its procedure as providing the backup data from the storage location (e.g., user service bureau) to a *second device*, which in some implementations is a new device – a replacement for the user's first

device. See (Cheng) APPL-1008, FIG. 4A, FIG. 5, [0009], [0046] – [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.” (Cheng) APPL-1008, [0048]. See also, (Cheng) APPL-1008, FIGS. 4A-4C, [0009], [0031] – [0039], [0045] – [0050].

144. A POSITA would recognize that applying Cheng’s teachings to Kesanupalli would provide a benefit. In particular, backing up data including at least one record of Kesanupalli to a second device allows for the user to save resources (e.g., time) in redeveloping the data in the record (e.g., biometric template and/or user credential). Use of Cheng provides for protecting the data in a secure method through Cheng’s two-tier encryption.

145. Second, it would have been obvious to *initiate backup* of a portion of the record to a second device as taught in Cheng based at least in part based on the *first device being a same brand as a second device* in light of teachings of Kodama. Like Cheng, Kodama also teaches a first user device, a backup service controlling the backup procedure, and a second user device, and a procedure of backing up data of the first user device to a second device. (Kodama) APPL-1010, (57), [0034], [0040]-[0041], [0101], [0106], FIG. 13 describing the backup procedure.

146. Just like in Cheng, Kodama teaches registering a first device with a

backup service, and Kodama continues to explain that this registration includes “device information including the manufacturer name, model name ...” (Kodama) APPL-1010, [0101]. A POSITA would understand that the “manufacturer name, model name” of a device provide a *brand* of a second device. Kodama’s backup service “adds the received information to the backup device registration table.” (Kodama) APPL-1010, [0103]. *See also*, (Kodama) APPL-1010, [0078] – [0104], FIG. 4 illustrating example backup device registration table with “manufacturer name 0403, a model number 0404, [0054], FIG. 6, “example of the device information. This table is configured from a manufacturer name 0601, a model number 0602...and is used upon registering the backup device in the online backup service system,” [0061]. Kodama then continues the backup process by sending a copy of the data of the registered first device (noted as 0105 in Kodama) to the backup service. (Kodama) APPL-1010, [0106] – [0107]. *See also*, (Kodama) APPL-1010 [0108] – [0118]. Thus, Kodama teaches providing a brand of the first device to the backup service.

147. Kodama continues its procedure by providing a *second device* that is associated with the user, registered with the backup service, and a target device for the backed-up data of the first device. In an example, the second device is a “new” device (device 0116) of the user. (Kodama) APPL-1010, [0160]. *See also*, (Kodama) APPL-1010 [0157], [0137]. In Cheng, the downloading or restoration

of the stored backup data onto the second device includes “verifying registration information of the user with a user service bureau.” (Cheng) APPL-1008, [0032]. *See also*, (Cheng) APPL-1008, FIG. 4A, [0047]. Kodama expands on this registration providing that the “device information including the manufacturer name, model name and product serial number” of the second device are read and sent to the backup service system. (Kodama) APPL-1010, [0135] – [0136]. The backup service system then “checks whether there is an entry where the user account name, device name and device information coincides.” (Kodama) 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.” (Kodama) APPL-1010 [0138]. In other words, only if the manufacturer name or model number, which are each a brand, of the second device is the same as the first device, the backup data is restored to the second device. *See also*, (Kodama) APPL-1010, [0143]-[0144]. Thus Kodama discloses initiating backup data onto a second device only if the brand of the second device is the same as the first device.

148. Thus, Kesanupalli, Cheng and Kodama render this element obvious.

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

149. Kesanupalli discloses *a memory coupled to the one or more processors*

and configured to provide the one or more processors with instructions.

150. Kesanupalli's system includes a main memory, a *memory*. (Kesanupalli) APPL-1006, 10:58-11:47 ("Main memory is also usually included for storing and retrieving larger amounts of information such as data and software applications configured to perform functions according to the invention when executed by the central processing unit.")

151. A 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*. As discussed above, the one or more processors includes circuitry executing the functions of the Host PC 202. A POSITA would understand that these functions are provided to the processor as *instructions*. See, e.g., (Kesanupalli) APPL-1006, claim 26. Kesanupalli explains that the application 112, such as Internet browser applications, "executes on a post PC 102." (Kesanupalli) APPL-1006, 5:59-66. An application executing on a PC requires instructions for its execution to be stored in a memory.

152. Thus, Kesanupalli teaches this element.

153. Therefore, Claim 1 is obvious over Kesanupalli, Cheng and Kodama.

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.

154. Kesanupalli, Cheng and Kodama render obvious claim 1 and

Kesanupalli discloses *second device is used to authenticate the user to one or more external resources*.

155. 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. (Kesanupalli) APPL-1006, 2:39-64, FIGS. 2, 7, 9, 11-12. That is, when accessing the external resource (website) with the second device, the user would authenticate herself to the website using the biometric authentication techniques of Kesanupalli. See, e.g., (Cheng) APPL-1008, [0022], [0050] (“new biometrics-based authentication device is available for use.”), (Kesanupalli), APPL-1006, FIG. 9.

156. 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.

157. Kesanupalli, Cheng and Kodama render obvious claim 1 and Kesanupalli and Cheng render obvious this further limitation.

158. 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." (Cheng) APPL-1008, [0022] ("[o]nboard **microprocessor** and communication means [] handle communication...and other **processing needs** such as establishing a **secure connection** with a remote service bureau, requesting and returning encryption/decryption keys, creating and copying lower tier and upper tier backup files, and terminating the connection.") For example, 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**." (Cheng) APPL-1008, [0048]. See also, (Cheng) APPL-1008, FIGS. 4A-4C, [0009], [0031]–[0039] (restoration). A secure connection is a *secure channel*. A POSITA would understand that a secure channel is a mechanism to pass data between two endpoints that has been secured from eavesdropping and manipulation by external parties (e.g., an encrypted network connection between two computers). A POSITA would further understand that a secure channel is created when secure connection is established (as described by Cheng, [0022]) between the endpoints of the user device and the remote service bureau.

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

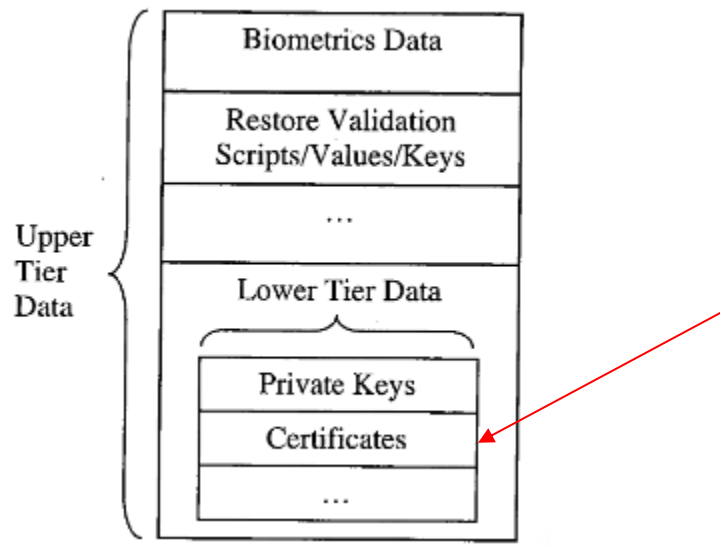
8. Claim 12

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

160. Kesanupalli, Cheng and Kodama render obvious claim 1 and Cheng's backup causes *a certificate to be transmitted to the second device*.

161. As illustrated above, Cheng's backup procedure implemented on Kesanupalli's system provides for encrypted backup files to be *transmitted to a second device*. See limitations [1.8]. Cheng also discloses the transmitted data includes a *certificate*. (Cheng) 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:



(Cheng) APPL-1008, FIG. 1

162. Kesanupalli describes:

Typical user authentication systems and procedures use passwords to authenticate the identity of the user. In many instances, Web sites are authenticated using SSL (Secure Sockets Layer) or other protocols. SSL is a protocol for securely transmitting information via the Internet. When using SSL, a Web site is authenticated via its certificate. The user seeking access to the Web site is then authenticated by username and password.

(Kesanupalli), APPL-1006, 1:37-34.

163. It is the practice of SSL to transmit certificates between endpoints to authenticate a first device or system to a second device or system, and vice-versa.

A certificate is a data structure that encodes a public key, wherein messages that are encrypted with a private key (known only to a single device) can be decrypted with the embedded public key found within the certificate. APPL-1031, (<https://www.ietf.org/rfc/rfc2246.txt>) “[Page 28]” discloses as part of the SSL/TLS Handshake Protocol overview: “Exchange certificates and cryptographic information to allow the client and the server to authenticate themselves.” See also, the standard directed to SSL protocol: “If the server is to be authenticated (which is generally the case), the server sends its certificate immediately following the server hello message.” APPL-1032 (The Secure Sockets Layer (SSL) Protocol Version 3.0, Section 5.6.2, Internet Engineering Task Force (IETF), Request for Comments: 6101, August 2011). Thus, a POSITA would recognize use of a certificate in cryptographic procedures such as described in Kesanupalli and Cheng (*e.g.*, encryption and decryption) would use a certificate containing a key that can encrypt or decrypt the files.

164. 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.

165. Kesanupalli, Cheng and Kodama render obvious claim 1 and Kesanupalli and Cheng render obvious this limitation.

166. 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.” ('105 patent), APPL-1001, 4:9-21, FIG. 2. See also, ('105 patent), APPL-1001, Figure 9.

167. As discussed above, Kesanupalli describes storing together a credential and a biometric template as a *record*. See limitation [1.3]. This data together with other associated information suggested by Kesanupalli (*e.g.*, user name, web site address) provides a *vault*. In particular, Kesanupalli illustrates at enrollment a user’s “Application ID[,] **User ID**[,] User Credential” along with the biometric data are provided for storage. (Kesanupalli) 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.” (Kesanupalli) 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.” (Kesanupalli) APPL-1006, 6:47-49. Thus, Kesanupalli describes storing in secure storage 206, a *vault* including, *e.g.*, data biometric template, credential, user ID, and an address for the associated external resource. A POSITA would expect a vault, such as that which Kesanupalli stores in secure storage 206, to include all of the security information that makes up the repository of the data, including the ciphertext. When copied to a different device

ciphertext would be different because it is going to be encrypted with a different set of keys. This and some other technical parts of the ciphertext (such as an encrypted initialization vector) would be changed each time it is exported to a new device. Accordingly, a POSITA would expect the version of the vault copied to a second device to be *modified* in that ciphertext and initialization vectors would be changed.

168. A POSITA would appreciate that the vault would contain version numbers to track when records are changed/copied/used. Versioning is a routine practice when creating any kind of replica of a database (which a vault definitely is). The version number allows a system to later reconcile changes at different devices, e.g., if one biometric template is updated on a device the vault would have a later version number than others. When the vaults are later reconciled (across devices), the older version would be replaced with the newer version. This is a basic function of any database backup solution and was routine practice before the earliest priority date. Moreover, a POSITA would understand that like most other authentication databases, the vault would include usage information for each credential/template (e.g., last accessed, last rejected). This again was a common feature of any authentication process, including those involving biometrics, before the earliest priority date. Usage information is used to manage the system, e.g., to retire unused credentials, to flag when a number of failed attempts have been used,

etc. For these reasons as well, a POSITA would expect the version of the vault copied to a second device to be *modified* in that versioning and use data would be changed. Finally, in the Kesanupalli-Cheng-Kodama system, this data of the first device (a *vault*) is copied and then encrypted in a two-tier encryption of Cheng for transmitting to a second device (via the user service bureau). See limitation [1.8]. For this reason as well, a backup copy provided to the second device is *modified* from that stored in the first device as it is encrypted by Cheng's two-tier encryption technique. (Cheng) APPL-1008, FIGS. 3A-3B. Therefore, Kesanupalli and Cheng describe a *backup comprises copying a modified version of a vault to the second device*.

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

10. Claims 18, 21, 23, 31 and 34

170. The limitations of independent Claim 18, except the preamble of the claim are substantively identical to limitations of claims already addressed above, as correlated in the table below:

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

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

<i>a backup, to the second device, of at least a portion of the at least one record.</i>	
--	--

[18.0] A method, comprising:

171. To the extent the preamble is limiting, Kesanupalli in view of Cheng and Kodama disclose it. The citations above apply to a *device* as in Claim 1 and also to a *method*. (Kesanupalli) APPL-1006, 2:30-38 (“The systems and methods described herein relate to biometric authentication of users. ...”), 10:48-54, FIG. 8.

172. Claim 18 is obvious in light of Kesanupalli in view of Cheng and Kodama.

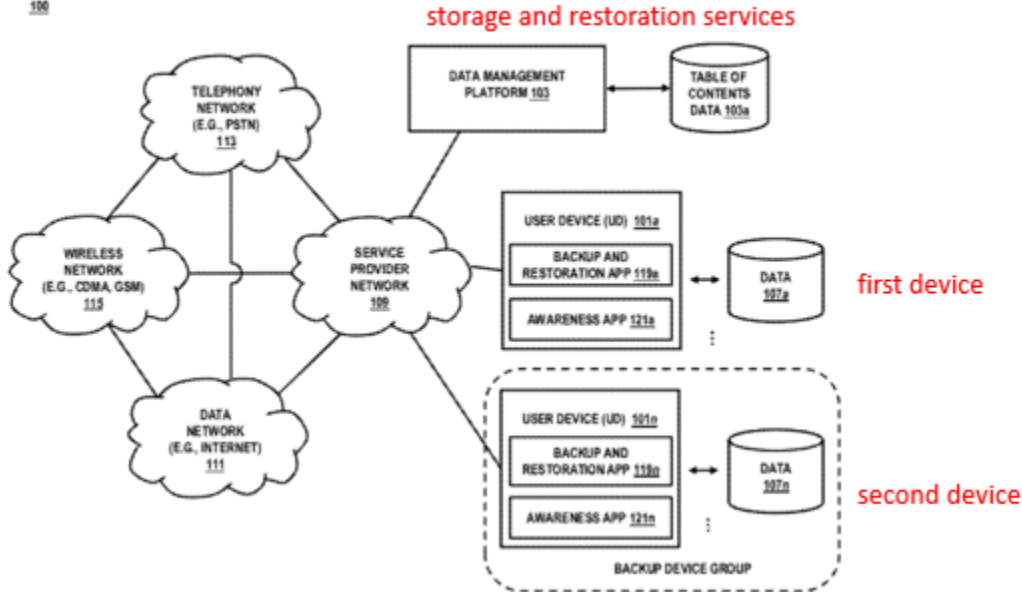
173. Dependent claims 21, 23, 31, and 34 are substantively identical to limitations discussed above, except that they depend from method claim 18 and thus are rendered obvious for the same reasons.

'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

174. 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. (Hubner) APPL-1030, (54), (57). 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. (Hubner) 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* (Hubner) APPL-1030, [0012], [0017]. Hubner “facilitate[s] the data restoration process based on the established physical presence of the user devices.” (Hubner) 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. (Hubner) 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. (Hubner) APPL-1030, [0017], [0026].

FIG. 1
100

(Hubner) APPL-1030, FIG. 1, annotated

2. Combination of Kesanupalli, Cheng, Kodama and Hubner

175. A 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. 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, which increases 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 (Hubner) APPL-1030, [0001], [0012]. The increased the opportunity for backup and restoration is particularly significant when/where wide-

area network (WAN) communications are unavailable or are bandwidth limited.

176. 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* VIII.4. (Hubner) APPL-1030, [0012], FIG. 1 “system 100” having user devices, network connections, 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* ('105 patent) APPL-1001, 11:54-12:3, 12:65-13:3, 14:23-25; (Hubner) APPL-1030, [0012]-[0015]. That is, a POSITA would recognize a reasonably pertinent problem faced by the inventor of the '105 patent would be addressing this backup of data without limiting transferring the backed-up data through an intermediary, which may be unavailable should communications with the intermediary (e.g., a network connection or gateway) or intermediary itself (e.g., a storage service) be unavailable, difficult or inconvenient to access by the user. To address this, a POSITA would be motivated to improve system designs, such as those relying exclusively on a wide-area network connection or cloud resources to support alternate means of performing their function where existing facilities are unavailable, e.g., during a WAN outage or server failure or simply when necessary wide area communication bandwidth is

unavailable or costly. Hubner's peer-to-peer technique would offer an independent communications to support backup or restore data traffic and thereby further enhance the backup facility of Kesanupalli/Cheng/Kodama. Considering independent failure modes and designing to include resilient data transfer option is a standard system design practice to make systems reliable in the face of environmental failures. Here, a POSITA would recognize systems designs using multiple independent channels to be more resilient in the face of failures and communication congestion. This approach—referred to in systems engineering as “independent failure modes”—was widely taught and used in designing software and hardware systems. Considering independent failure modes means engineering system designs to implement multiple independent channels to improve resilience of the system. *See, e.g.*, (Embracing Failure to Improve Resilience and Maximize Availability) APPL-1034 (discussion of building an application with redundancy and fault tolerance).

177. A 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. As discussed above in Section VIII.A.4, a POSITA would readily recognize a personal electronic device can be lost, damaged, or otherwise require replacement. *See*

(Kesanupalli) APPL-1006, 10:13-18; (Cheng) APPL-1008, [0006]; (Hubner) APPL-1030, [0001] (“This manual process may not be performed regularly enough by the user, however, to ensure the availability of relevant and timely copies of the data. Consequently, when data on the device is lost or corrupted, the user may simply have to incur the cost and inconvenience of acquiring the data again (assuming such option is even possible).”) 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. (Hubner) APPL-1030, [0001], [0012]; (Kesanupalli) APPL-1006, 10:13-18; (Cheng) APPL-1008, [0006]. A POSITA would have what Hubner recognizes as a lack of diligence of a user’s frequency in backing up data to mitigate her risk of loss of the data. (Hubner) APPL-1030, [0014]. Therefore, additional modes of “effective, convenient execution of data backup and restoration for user devices” are beneficial. (Hubner) APPL-1030, [0001]-[0002], [0012].

178. A 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. Adding peer-to-peer communications allows for backup data transfer that avoids a bottleneck at, or unavailability of, a WAN interface. *See, e.g.*, (pStore: A Secure

Peer-to-Peer Backup System), APPL-1035. 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*, (Cheng) APPL-1008, [0029]; *see also*, (Kesanupalli) 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. Engineering and designing systems to provide redundancy to address these limitations was well-known practice. *See*, e.g., APPL-1034, "Embracing Failure to Improve Resilience and Maximize Availability". 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] ("various signals detected by the integrated sensory systems of the peer user devices 101a-101n, including Bluetooth signals, WiFi broadcasts, audio signals, internet protocol (IP) stack data (e.g., IP address data) associated with a mutually configured local or wide area communication network, and any other signals or metrics produced as a result of range based communication protocols. As such, peer devices may detect each other's presence without indicating or identifying the end user."); [0026] ("is

noted, though not shown in the figure, that in certain embodiments user devices 101a-101 in may be configured to establish peer-to-peer communication sessions with each other using a variety of technologies—near field communication (NFC), Bluetooth, infrared, etc. Also, connectivity can be provided via a wireless local area network (LAN).”) For example, a POSITA would recognize instances where a user may not have access to or be bandwidth limited on an internet connection for transmitting data to an internet-based backup or storage service such as suggested in Cheng but have a local connection to a second user device such as through a local communication network, a private area network, Bluetooth signals, and other local, proximity based systems. See (Hubner), APPL-1030, [0023], [0026]. As discussed above, a POSITA would recognize systems designs using multiple independent channels such as also Bluetooth connectivity to be more resilient in the face of failures and communication congestion.

179. Another benefit a POSITA would recognize in applying Hubner’s technique of communicating data between peer-level devices is an increase in security. 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 itself be employed as an additional factor in a multifactor

authentication scheme to increase confidence in authentication of a target device or system. *See, e.g.*, (Hubner) APPL-1030, awareness application 121, [0016], [0017]; (Varshavsky), APPL-1036 (describing advantages of proximity based authentication of mobile devices). 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].

180. 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. (Hubner) 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. See ("Protecting File Systems: A Survey of Backup Techniques") APPL-1037. Further, a 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. The manufacturer of the same-brand devices typically ensures compatibility by using the same underlying implementations (or code bases), the same developers, and the same protocols. Moreover, the quality assurance departments of the brands would test the compatibility of these exchanges prior to releasing the products to the general public.

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.

181. 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.

182. 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 a 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. (’105 Patent) APPL-1001, 16:33-49. This is the same procedure as disclosed in Cheng, which 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 Cheng, FIG. 4A, [0032]-[0035]. Here, a POSITA would understand the steps “Online registration verification()”, “Verify registration detail()”, “Return Upper tier key()”, “Upload backup file()” and “Decrypt upper tier backup file()” of Figure 4A of Cheng would involve the passing of “certificate or another type of assurance” (e.g., password) to authenticate the second device to the User Service Bureau, receiving keys, and recover the plaintext authentication data to perform pairing. See (Cheng) APPL-1008, FIG. 4A. This is a substantially the same process as disclosed with respect to the exemplary pairing process of ’105 patent’s Figure 9. 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.

183. 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. A POSITA would understand peer-to-peer (P2P) pairing in the context of the '105 patent involves sources and targets of data to establish connections, perform mutual authentication, and securely transfer data. A POSITA would have found it obvious and simple to implement the Hubner's teachings on P2P as described above, for example, by simply changing the type of authentication of the source from an authentication mechanism (e.g., certificate) to a P2P service (e.g., as in the widely used Kerberos authentication system).¹⁰

184. 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.

In one embodiment, when one or more **peer user devices 101a-101n** are registered with the data management platform 103, they are able to **interact**

¹⁰ APPL-1033, <https://www.ietf.org/rfc/rfc4120.txt>

with one another for automatically invoking **data backup and restoration upon request**. By way of example, when user devices 101a-101n 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 awareness application 121 has visibility to the various signals detected by the integrated sensory systems of the peer user devices 101a-101n, including **Bluetooth signals**, WiFi broadcasts, audio signals, internet protocol (IP) stack data (*e.g.*, IP address data) associated with a mutually configured local or wide area communication network, and any other signals or metrics produced as a result of range based communication protocols. As such, **peer devices may detect each other's presence** without indicating or identifying the end user.

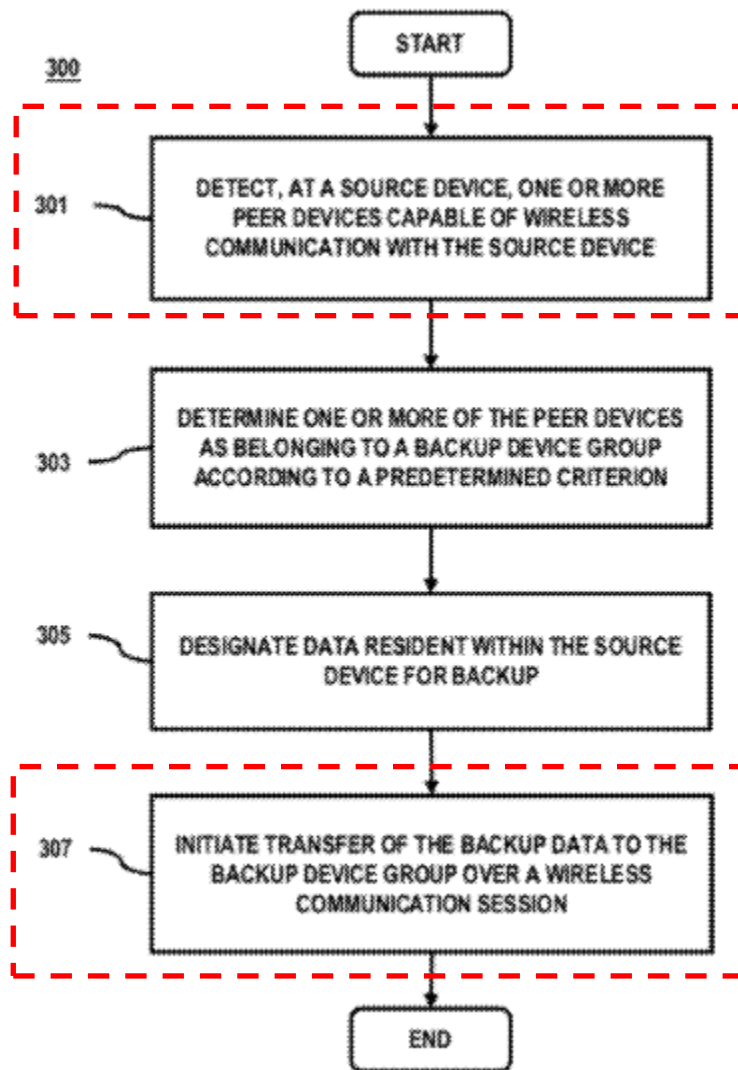
(Hubner) APPL-1030 [0017]. *See also*, [0026], [0031].

185. Bluetooth pairing mirrors the pairing description in the '105 patent. The creation of long-term associations between devices in Bluetooth is referred to as pairing. *See* (Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology) APPL-1038(describing pairing and Bluetooth security features). In this process, a first peer device (often called the master in the Bluetooth security mode descriptions) and second peer device (often

called a slave) discover each other via near-field communication by listening to local low-power radio communication. APPL-1038, 18 (simple secure pairing). Once discovered, the devices can perform mutual authentication (perhaps using a shared password, PIN or other interface). APPL-1038, 19-23 (shared secrets, PIN, public/private key pairs). The paired devices share addressing and other device-specific information, as well as establish cryptographic keys. The devices then use that information to establish and maintain a secure session.

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

FIG. 3A



APPL-1030, FIG. 3A

(Hubner) 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. (Hubner) APPL-1030, [0013].

187. 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.

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

189. 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." (Cheng) APPL-1008, [0009]. A POSITA would understand Cheng's registration process of 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. (Cheng) 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).

190. 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.” (Hubner) 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.” (Hubner) 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[.]” (Hubner) APPL-1030, [0031]. A 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. It is noted Hubner’s inputs for enrollment/authentication are the same as the *authentication inputs* discussed in the ’105 patent. (’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, a 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. Bluetooth supports several authentication methods during the pairing process. In one popular approach, a device such as a cell phone will display a 4-digit PIN that can be entered in the other pairing device and used to generate symmetric keys. APPL-1038, 17-18 (security modes 2 and 3). If the PIN is correctly entered, it is deemed authentic and the pairing can proceed. Other modes used pre-programmed or real-time entered shared secrets (e.g., passwords, cryptographic keys), or the devices securely negotiate secrets over the wireless connection using complex cryptographic methods (e.g., over an Elliptic-Curve Diffie Hellman exchange). APPL-1038, 18-19 (secure simple pairing and security mode 4). In all these modes, the authentication step of the pairing process pairing process comprises a comparison of data generated from one or more authentication inputs, whether they be entered, configured or established via cryptographic protocol. See APPL-1038, 19-21 (describing authentication).

191. 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* (Kesanupalli) APPL-1006, 1:35-46, 2:30-48, FIGS. 7, 9. A 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.

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

5. Claims 24 and 25

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

C. Ground 3: Claims 1, 2, 4, 12, 15, 18, 21, 23, 31, and 34 are obvious under 35 U.S.C. § 103 over Jakobsson 351 and Kodama.

1. Jakobsson 351 and Kodama

194. Jakobsson 351 is an issued patent stemming from U.S. Application No. 15/042,636, which is an application to which the '105 patent claims priority (through a CIP). As noted above, Jakobsson 351 does not contain written description of the Challenged Claims of the '105 patent as particularly 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. See Section V. Kodama discloses this element and would be obvious to combine with Jakobsson 351; Kodama is discussed above at Section VIII.A.3.

2. Reasons to Combine Jakobsson 351 and Kodama

195. For similar reasons as discussed above with respect to Kesanupalli and Kodama as discussed in Section VIII.A.4, it would have been obvious to combine Jakobsson 351 and Kodama. In particular, a POSITA would have motivated to apply Kodama’s teachings of ensuring devices in the backup technique of Jakobsson 351 are of the same brand, which provides the obvious, beneficial and predictable result of mitigates complexity, compatibility and security issues. I explain this further here. First, this allows the developer of the system to rely on brand specific implementations that ensure that all devices in a

product line can leverage the backup service (compatibility) with minimal interfaces tailored to the homogeneous interface design (complexity). This results in a small, closed source (not public) design and codebase that uses credentials and cryptographic keys that need only be created and known to the manufacturer—and thus provides strong security.

196. First, Jakobsson 351 and Kodama are in the same field of endeavor. Each reference is directed to an environment of a plurality of devices such as client devices and backup systems interacting over a network. (Jakobsson 351) APPL-1011, FIG. 1; (Kodama) APPL-1010, FIG. 1; ('105 patent) APPL-1001, FIG. 1. Each are also concerned with transfer, protection, and back up of data associated with the devices of the environment. (Kodama) APPL-1010, [0040], [0041], [0159]; (Jakobsson 351) APPL-1011, 12:13-20; ('105 patent) APPL-1001, 1:43-50. As Jakobsson 351 is within the priority chain of the '105 patent it is evident that 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. (Kodama) 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.” As evidenced on the front page of Jakobsson 351, the '105 patent, and Kodama, the international classification (IPC), U.S. classifications (CPC) and/or the field of search

classification consulted by the Office during examination for each patent include the same subclass, namely CPC/IPC G0F6 21 (security arrangements for protecting computers, components thereof, programs or data against unauthorized activity). See ('105 patent) APPL-1001, (51), (52); (Jakobsson 351) APPL-1011, (52), (Kodama) APPL-1010, (51).

197. Second, a POSITA would have found it predictable to apply Kodama's teachings to Jakobsson 351's backup process. Jakobsson 351 describes the desire to back up or synchronize data across a user's devices including "(e.g., 102 and 104)," which can include devices of different types. (Jakobsson 351) APPL-1011, 7:37-41. However, Jakobsson 351 does not consider properties of the synchronized devices that may affect this synchronization. Kodama recognizes "if data restoration is to be performed to a different product or a different manufacturer, the format and product proprietary information of data between the products will differ." (Kodama) APPL-1010, [0157]. A POSITA would recognize an advantage of basing initiating the transfer of data at least in part on a brand to avoid the compatibility issues as highlighted by Kodama. As highlighted above, developing proprietary backup solutions for a product line can reduce complexity, ensure compatibility among devices in that line, and be more secure. A manufacturer of a device including an authentication system implements a proprietary system that frequently includes different features, perform slightly

different template matching, support different biometric sensors (e.g., fingerprint sensors), and store different kinds of credentials. Such features act as market differentiators and are used in advertising to entice customers (i.e., users or system manufacturers) to purchase these devices over competitor offerings. Differences in features and algorithms would also necessitate that the fingerprint/credential database be tailored to these custom systems by containing a unique combination of data fields and other structures. Kodama describes that its methods and system are “capable of mitigating the risk of a third party referring to or using backup data without authorization upon restoring such backup data in an electronic appliance.” (Kodama) APPL-1010, [0007]. One way it ensures this benefit is by ensuring the originating device and the restoration device are the same brand and have sufficient compatibility.

198. A POSITA would have also had a reasonable expectation of success. Kodama states that: “Conventionally, technology of backing up data in a PC to an external recording medium, replacing the HDD when the HDD in the PC malfunctions, and restoring the backed-up data in the PC is widely known. Remote copy technology of copying data among storage apparatuses is also widely known.” (Kodama) APPL-1010, [0003]. Providing a check in the systems and methods performing the back up of a brand is a simple addition of routine software executed on generic processing components. Kodama’s teachings are

implemented by a small addition of one or more fields to that routine software executed on generic processing components.

3. Claim 1

a) [1.0] *A system, comprising:*

199. Jakobsson 351 provides a claim 1 directed to *a system*. “1. A system, comprising:” (Jakobsson 351) APPL-1011, 10:50. As described below, this system provides the same elements of Claim 1 of the ’105 patent.

200. Thus, Jakobsson 351 discloses this element.

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

201. Jakobsson 351 at claim 1 recites its system comprises “one or more processors configured to[.]” (Jakobsson 351) APPL-1011, 10:51.

202. Thus, Jakobsson 351 discloses this element.

c) [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;*

203. Jakobsson 351 at claim 1 recites its system comprises the processors are 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; ...” (Jakobsson 351) APPL-1011, 10:52-55. The resource is associated with the user as it is requested by the user.

204. Thus, Jakobsson 351 discloses this element.

d) **[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,***

205. Jakobsson 351 at claim 1 recites its system comprises the processors are configured to:

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

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

(Jakobsson 351) APPL-1011, 10:56-11:3. The system of claim 1 also uses a “template” for its match, which 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.” (Jakobsson 351) APPL-1011, 11:22-24, 12:8-12. See also, (Jakobsson 351) APPL-1011, 11:45-56, FIG. 2.

206. Thus, Jakobsson 351 discloses this element.

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

207. Jakobsson 351 at claim 1 recites: “wherein the previously stored credential retrieved from the record stored on the device comprises at least one of a cryptographic key and a cookie.” (Jakobsson 351) APPL-1011, 11:1-3.

208. Thus, Jakobsson 351 discloses this element.

f) [1.4] *receive authentication input from the user;*

209. Jakobsson 351 at claim 1 recites the 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.” (Jakobsson 351) APPL-1011, 10:51-55.

210. Thus, Jakobsson 351 discloses this element.

g) [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;*

211. Jakobsson 351 continues to recite in its claim 1 that its one or more processors of the system:

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

(Jakobsson 351) APPL-1011, 10:56-60. *See also*, (Jakobsson 351) APPL-1011, 11:45-50, FIG. 2, 4:55-68.

212. Thus, Jakobsson 351 discloses this element.

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

213. Jakobsson 351 continues to recite in its claim 1 that its one or more processors of the system:

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

(Jakobsson 351) APPL-1011, 10:61-11:30. *See also*, (Jakobsson 351) APPL-1011, 12:4-7.

214. Thus, Jakobsson 351 discloses this element.

i) [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*

215. Jakobsson 351 continues to recite in its claim 1 that its one or more

processors of the system:

establish a connection between the device and the external resource to which the user requested access; and
facilitate a login of the user to the external resource at least in part by transmitting, on behalf of the user, from the device and via the established connection, output based at least in part on the at least one of the cryptographic key and the cookie retrieved from the record accessed at least in part by determining, by the authentication translator at the device, the matching using the received authentication input, wherein the user of the device is logged into the external resource based at least in part on the output transmitted from the device on behalf of the user

(Jakobsson 351) APPL-1011, 11:4-18.

216. Thus, Jakobsson 351 discloses this element.

j) ***[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***

217. Jakobsson 351 in view of Kodama teaches element [1.8].

218. Jakobsson 351 continues to recite in its system and its:

processors are further configured to:

encrypt and authenticate at least a portion of the record; and

perform a backup of the encrypted and authenticated record to a remote

storage entity, wherein the remote storage entity is configured to synchronize records between at least two devices associated with the user.

(Jakobsson 351) APPL-1011, 12:13-20.

219. It would have been obvious to initiate this 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*.

220. Like Jakobsson 351, Kodama also teaches a first user device, a backup service controlling the backup procedure, and a second user device, and a procedure of backing up data of the first user device to a second device that is controlled by the backup service (“remote storage entity” in Jakobsson 351).

221. Kodama teaches registering a first device with a backup service, and Kodama continues to explain that this registration includes “device information including the manufacturer name, model name ...” (Kodama) APPL-1010, [0101]. A POSITA would understand that the “manufacturer name, model name” of a device provide a *brand* of a second device. Kodama’s backup service “adds the received information to the backup device registration table.” (Kodama) APPL-1010 [0103]. *See also*, (Kodama) APPL-1010 [0078] – [0104], FIG. 4 illustrating example backup device registration table with “manufacturer name 0403, a model number 0404, [0054], FIG. 6, “example of the device information. This table is configured from a manufacturer name 0601, a model number 0602...and is used

upon registering the backup device in the online backup service system,” [0061].

Kodama then continues the backup process by sending a copy of the data of the registered first device (noted as 0105 in Kodama) to the backup service. (Kodama) APPL-1010 [0106] – [0107]. *See also*, (Kodama) APPL-1010 [0108] – [0118].

Thus, Kodama teaches providing a brand of the first device to the backup service.

222. Kodama continues its procedure by providing a *second device* that is associated with the user, registered with the backup service, and a target device for the backed-up data of the first device. In an example, the second device is a “new” device (device 0116) of the user. (Kodama) APPL-1010, [0160]. *See also*, (Kodama) APPL-1010 [0157], [0137]. Kodama describes that a second device registers with the backup service by providing that the “device information including the manufacturer name, model name and product serial number” of the second device are read and sent to the backup service system. (Kodama) APPL-1010, [0135] – [0136]. The backup service system then “checks whether there is an entry where the user account name, device name and device information coincides.” (Kodama) 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.” (Kodama) APPL-1010 [0138]. In other words, only if the manufacturer name or model number of the second device

is the same as the first device, the backup data is restored to the second device. *See also*, (Kodama) APPL-1010 [0143]-[0144]. A POSITA would understand at least “manufacturer name” of a device functions as a *brand* of a second device. Thus Kodama discloses initiating backup data onto a second device only if the brand is of the second device is the same as the first device.

223. Thus, Jakobsson 351 and Kodama teach this element.

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

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

225. Thus, Jakobsson 351 discloses this element.

226. Therefore, Claim 1 is obvious over Jakobsson 351 and Kodama.

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.

227. Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation.

228. 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.

229. 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.

230. Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation.

231. Jakobsson '351 suggests a user device communicates with a cloud storage service to keep the authentication information synchronized.

(Jakobsson '351) 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.”

(Jakobsson '351) APPL-1011, 4:67-5:3 (describing a secure connection between a user device and website).

232. 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.

233. Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and POSITA would have found it obvious to include a certificate.

234. Jakobsson '351 describes communication of a credential associated with a website for backup (see [1.8]) and Jakobsson '351 further recognizes communication between the user device and a service provider is over an SSL connection. (Jakobsson '351) APPL-1011, 5:1-3, 5:43-6:5. POSITA would recognize including in the authentication data associated with a website accessed by SSL, as described in Jakobsson '351, a *certificate* would have been obvious. This is because a POSITA recognizes SSL communication includes an SSL certificate that authenticates a website's identity and enables a secure connection. It is the practice of SSL to transmit certificates between endpoints to authenticate a first device or system to a second device or system, and vice-versa. A certificate is a data structure that encodes a public key, wherein messages that are encrypted with a private key (known only to a single device) can be decrypted with the embedded public key found within the certificate (<https://www.ietf.org/rfc/rfc2246.txt>) "[Page 28]" discloses as part of the SSL/TLS Handshake Protocol overview: "Exchange certificates and cryptographic information to allow the client and the server to authenticate themselves." Thus,

POSITA would recognize use of a certificate in cryptographic procedures of Jakobsson '351 (*e.g.*, encryption and decryption) would use a certificate containing a key that can encrypt or decrypt the files. 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.

235. 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.

236. Jakobsson '351 and Kodama render obvious all the limitations of claim 1 and also this limitation.

237. 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.” (Jakobsson '351) 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. (Jakobsson '351) APPL-1011, 7:2-10.

Moreover, for each the changed ciphertext and updated version tracking and usage data reasons detailed above with respect to Claim 15 and Ground 1 (see ¶¶167-168), POSITA would expect the version of a vault copied to a second device to be a *modified* version.

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

8. Claims 18, 21, 23, 31, 34

239. The limitations of independent Claim 18, except the preamble of the claim, are substantively identical to limitations of claims already addressed above. Jakobsson 351 similarly includes a method claim 17, which is substantially similar to the cited system of claim 1 of Jakobsson 351 discussed above. The chart below illustrates the citations of Jakobsson 351, which apply to Claim 18 in conjunction with the citations and analysis discussed with respect to Jakobsson 351's claim 1 above.

Claim 18 Limitation	Disclosure of Jakobsson 351	Corresponding Claim Limitation discussed above
[18.0] <i>A method, comprising:</i>	(Jakobsson 351) APPL-1011, 12:21	
[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>	(Jakobsson 351) APPL-1011, 12:22 - 25	[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>	(Jakobsson 351) APPL-1011, 12:26-39, 56-58	[1.3]
[18.3] <i>receiving authentication input from the user;</i>	(Jakobsson 351) APPL-1011, 12:22 - 25	[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>	(Jakobsson 351) APPL-1011, 12:26-30	[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>	(Jakobsson 351) APPL-1011, 12:31-39	[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>	(Jakobsson 351) APPL-1011, 12:40-53	[1.7]
[18.7a] <i>based at least in part on the first device being a same brand as a second device,</i>	As to [18.7b], (Jakobsson 351) APPL-	[1.8]

[18.7b] <i>initiating a backup, to the second device, of at least a portion of the at least one record.</i>	1011, 14:16-22	
---	----------------	--

240. Thus, Claim 18 is obvious in light of Jakobsson 351 and Kodama.

241. Dependent Claims 21, 23, 31, and 34 depend from claim 18 and are substantively identical to dependent claims already addressed above, as correlated in the table below. The combination of Jakobsson 351 and Kodama renders obvious these claims for the same reasons discussed above with respect to Claim 18 and the corresponding claims in of the table.

'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

242. Hubner is discussed at Section VIII.B.1.

2. Combination of Jakobsson '351, Kodama and Hubner

243. A 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. Jakobsson '351 having 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, which increases 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* (Hubner) APPL-1030, [0001], [0012]. The increased the opportunity for backup and restoration is particularly significant when/where wide-area network (WAN) communications are unavailable or are bandwidth limited.

244. Hubner is in the same field of endeavor as Jakobsson '351 as enhanced by the Kodama and the '105 patent, such as security arrangements and procedures for transferring and protecting data in computer systems. *See supra* VIII.4. (Hubner) APPL-1030, [0012], FIG. 1 "system 100" having user devices, network connections, 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* ('105 patent) APPL-1001, 11:54-12:3, 12:65-13:3, 14:23-25; (Hubner) APPL-1030, [0012]-[0015]. That is, a POSITA would recognize a reasonably pertinent problem faced by the inventor of the '105 patent would be addressing this backup of data without

limiting transferring the backed-up data through an intermediary, which may be unavailable should communications with the intermediary (e.g., a network connection or gateway) or intermediary itself (e.g., a storage service) be unavailable, difficult or inconvenient to access by the user. To address this, a POSITA would be motivated to improve system designs, such as those relying exclusively on a wide-area network connection or cloud resources to support alternate means of performing their function where existing facilities are unavailable, e.g., during a WAN outage or server failure or simply when necessary wide area communication bandwidth is unavailable or costly. Hubner's peer-to-peer technique would offer an independent communications to support backup or restore data traffic and thereby further enhance the backup facility of Jakobsson '351/Kodama. Considering independent failure modes and designing to include resilient data transfer option is a standard system design practice to make systems reliable in the face of environmental failures. Here, a POSITA would recognize systems designs using multiple independent channels to be more resilient in the face of failures and communication congestion. This approach—referred to in systems engineering as “independent failure modes”—was widely taught and used in designing software and hardware systems. Considering independent failure modes means engineering system designs to implement multiple independent channels to improve resilience of the system. *See, e.g.,*

(Embracing Failure to Improve Resilience and Maximize Availability) APPL-1034 (discussion of building an application with redundancy and fault tolerance).

245. A POSITA would have been motivated to employ Hubner's peer-to-peer technique of backing up and restoring data in connection with Jakobsson '351 having 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. As discussed above in Section VIII.A.4, a POSITA would readily recognize a personal electronic device can be lost, damaged, or otherwise require replacement. *See* (Hubner) APPL-1030, [0001] ("This manual process may not be performed regularly enough by the user, however, to ensure the availability of relevant and timely copies of the data. Consequently, when data on the device is lost or corrupted, the user may simply have to incur the cost and inconvenience of acquiring the data again (assuming such option is even possible).") Hubner recognizes what a 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. (Hubner) APPL-1030, [0001], [0012]. A POSITA would have understood what Hubner recognizes as a lack of diligence of a user's frequency in backing up data to mitigate her risk of loss of the data. (Hubner) APPL-1030, [0014]. Therefore, additional modes of “effective, convenient execution of data backup and restoration for user devices” are beneficial. (Hubner) APPL-1030,

[0001]-[0002], [0012].

246. A 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. Adding peer-to-peer communications allows for backup data transfer that avoids a bottleneck at, or unavailability of, a WAN interface. *See, e.g.,* (pStore: A Secure Peer-to-Peer Backup System), APPL-1035. 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 cloud storage service. *See, (Jakobsson '351) 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. Engineering and designing systems to provide redundancy to address these limitations was well-known practice. *See, e.g., APPL-1034, "Embracing Failure to Improve Resilience and Maximize Availability".* 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] ("various signals detected by the integrated sensory systems of the peer user devices 101a-101n,

including Bluetooth signals, WiFi broadcasts, audio signals, internet protocol (IP) stack data (e.g., IP address data) associated with a mutually configured local or wide area communication network, and any other signals or metrics produced as a result of range based communication protocols. As such, peer devices may detect each other's presence without indicating or identifying the end user."); [0026] ("is noted, though not shown in the figure, that in certain embodiments user devices 101a-101 in may be configured to establish peer-to-peer communication sessions with each other using a variety of technologies—near field communication (NFC), Bluetooth, infrared, etc. Also, connectivity can be provided via a wireless local area network (LAN).") For example, a POSITA would recognize instances where a user may not have access to or be bandwidth limited on an internet connection for transmitting data to a cloud based service suggested in Jakobsson '351 but have a local connection to a second user device such as through a local communication network, a private area network, Bluetooth signals, and other local, proximity based systems. See (Hubner), APPL-1030, [0023], [0026]. As discussed above, a POSITA would recognize systems designs using multiple independent channels such as also Bluetooth connectivity to be more resilient in the face of failures and communication congestion.

247. Another benefit a POSITA would recognize in applying Hubner's technique of communicating data between peer-level devices is an increase in

security. 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 itself be employed as an additional factor in a multifactor authentication scheme to increase confidence in authentication of a target device or system. *See, e.g.*, (Hubner) APPL-1030, awareness application 121, [0016], [0017]; (Varshavsky), APPL-1036 (describing advantages of proximity based authentication of mobile devices). 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].

248. 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 enhanced with 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 cloud service of Jakobsson ’351. (Hubner) 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 Jakobsson ’351’s system and devices. See (“Protecting File Systems: A Survey of Backup Techniques”) APPL-1037. Further, a 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. The manufacturer of the same-brand devices typically ensures compatibility by using the same underlying implementations (or code bases), the same developers, and the same protocols. Moreover, the quality assurance departments of the brands would test the compatibility of these exchanges prior to releasing the products to the general public.

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.

249. Claim 1 is rendered obvious by Jakobsson ’351 and Kodama and

claim 5 is rendered obvious by Jakobsson '351, Kodama and Hubner. Hubner describes a system that provides for a first device and a second device to be configured to complete a *pairing process*.

250. 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.

In one embodiment, when one or more **peer user devices 101a-101n** are registered with the data management platform 103, they are able to **interact with one another** for automatically invoking **data backup and restoration upon request**. By way of example, when user devices 101a-101n 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 awareness application 121 has visibility to the various signals detected by the integrated sensory systems of the peer user devices 101a-101n, including **Bluetooth signals**, WiFi broadcasts, audio signals, internet protocol (IP) stack data (*e.g.*,

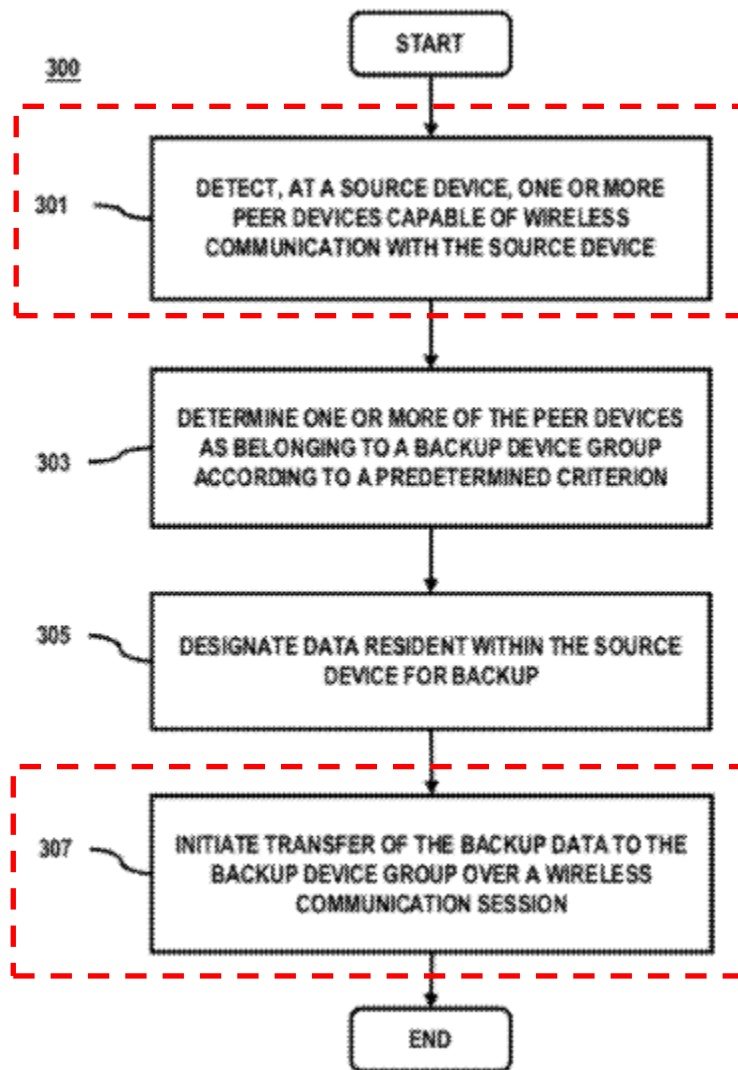
IP address data) associated with a mutually configured local or wide area communication network, and any other signals or metrics produced as a result of range based communication protocols. As such, **peer devices may detect each other's presence** without indicating or identifying the end user.

(Hubner) APPL-1030 [0017]. *See also*, [0026], [0031].

251. Bluetooth pairing mirrors pairing description in the '105 patent. The creation of long-term associations between devices in Bluetooth is referred to as pairing. *See* (Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology) APPL-1038(describing pairing and Bluetooth security features). In this process, a first peer device (often called the master in the Bluetooth security mode descriptions) and second peer device (often called a slave) discover each other via near-field communication by listening to local low-power radio communication. APPL-1038, 18 (simple secure pairing). Once discovered, the devices can perform mutual authentication (perhaps using a shared password, PIN or other interface). APPL-1038, 19-23 (shared secrets, PIN, public/private key pairs). The paired devices share addressing and other device-specific information, as well as establish cryptographic keys. The devices then use that information to establish and maintain a secure session.

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

FIG. 3A

**APPL-1030, FIG. 3A**

(Hubner) 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 Jakobsson '351 enhanced by Kodama system. (Hubner) APPL-1030, [0013].

253. 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.

254. Claim 6 is obvious over Jakobsson '351, Kodama and Hubner.

255. 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.

256. 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.”

(Hubner) 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.” (Hubner)

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[.]” (Hubner) APPL-1030, [0031]. A 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. It is noted Hubner’s inputs for enrollment/authentication are the same as the *authentication inputs* discussed in the ’105 patent. (’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, a 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. Bluetooth supports several authentication methods during the pairing process. In one popular approach, a device such as a cell phone will display a 4-digit PIN that can be entered in the other pairing device and used to generate symmetric keys. APPL-1038, 17-18 (security modes 2 and 3). If the PIN is correctly entered, it is deemed authentic and the pairing can proceed. Other modes used pre-programmed or real-time entered shared secrets (*e.g.*, passwords,

cryptographic keys), or the devices securely negotiate secrets over the wireless connection using complex cryptographic methods (e.g., over an Elliptic-Curve Diffie Hellman exchange). APPL-1038, 18-19 (secure simple pairing and security mode 4). In all these modes, the authentication step of the pairing process pairing process comprises a comparison of data generated from one or more authentication inputs, whether they be entered, configured or established via cryptographic protocol. See APPL-1038, 19-21 (describing authentication).

257. To the extent Patent Owner argues the authentication input is a biometric input and the comparison is with a biometric template, implementing a biometric authentication would have been obvious in light of Jakobsson '351 and Kodama. A POSITA would have found it obvious to increase the security of Hubner's pairing process by biometric authentication, a well-known authentication technique. See Section VI.A. Biometric authentication techniques can enhance security.

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

5. Claims 24-25

259. 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.

IX. CONCLUSION

This declaration and my opinions herein are made to the best of my knowledge and understanding, and based on the material available to me, at the time of signing this declaration. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 or Title 18 of the United States Code.



Date: January 31, 2024 _____