UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

APPLE INC,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

_____

IPR2023-00333
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....6

II. Qualifications and Professional Experience....8

III. Level of Ordinary Skill in the Art....12

IV. Relevant Legal Standards....14

V. Overview of the '105 Patent....18

VI. Technology Background....27

A. AUTHENTICATION....27

B. CREDENTIALS AND CREDENTIAL MANAGEMENT....28

C. CRYPTOGRAPHY....32

D. CRYPTOGRAPHY IN WEB TRANSACTIONS....33

E. TRUSTED PLATFORM MODULES....34

VII. Claim Construction....36

A. "*restricted interface" (Claims 9-11 and 28-30)*....37

VIII. Claims 1, 9-11, 14, 18, 28-30, 33 and 35 are Unpatentable....38

A. Ground 1: Claims 1, 14, 18, 33, and 35 are obvious under 35 U.S.C. § 103 over Kesanupalli, Cheng and Kodama....40

1. Summary of Kesanupalli....40

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] *one or more processors configured to:* 57

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;* 59

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,*.....64

e) [1.3b] *wherein the credential information comprises a cryptographic key;*.....72

f) [1.4] *receive authentication input from the user;* 74

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;*.....75

h) [1.6] *retrieve at least a portion of the credential information from the at least one record stored on the first device;* 78

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* 80

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* 84

k) [1.9] *a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.*.....88

6. Claim 14 89

7. Claims 18 and 33 90

8. Claim 35 92

B. Ground 2: Claims 9-11 and 28-30 are obvious under 35 U.S.C. § 103 over Kesanupalli, Cheng, and Kodama and in further view of Challener. 94

1. Summary of Challener 94

2. Reasons to Combine Kesanupalli in view of Cheng and Kodama and Challener 99

3. Claim 9 103

4. Claim 10 108

5. Claim 11 109

6. Claims 28-30 109

C. Ground 3: Claims 1, 9-11, 14, 18, 28-30, 33 and 35 are obvious under 35 U.S.C. § 103 over Jakobsson 351 and Kodama. 111

1. Jakobsson 351 and Kodama 111

2. Reasons to Combine Jakobsson 351 and Kodama 111

3. Claim 1 115

a) [1.0] *A system, comprising*: 115

b) [1.1] *one or more processors configured to*: 115

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*; 115

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,* 116

e) [1.3b] *wherein the credential information comprises a cryptographic key*;.....117

f) [1.4] *receive authentication input from the user*;.....117

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*;.....117

h) [1.6] *retrieve at least a portion of the credential information from the at least one record stored on the first device*; 118

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* 118

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* 119

k) [1.9] *a memory coupled to the one or more processors and configured to provide the one or more processors with instructions.* 122

4. Claim 9 122

5. Claim 10 123

6. Claim 11 124

7. Claim 14 125

8. Claims 18, 28-30, and 33 125

9. Claim 35 127

IX. Conclusion 130

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, 9-11, 14, 18, 28-30, 33, and 35 ("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; and

g) 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, *Authentication*, 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-1021	Redline comparison of U.S. Patent No. 10,360,351 patent specification and the '105 patent
APPL-1023	RFC2818, HTTP Over TLS (May 2000)
APPL-1024	https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf

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 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

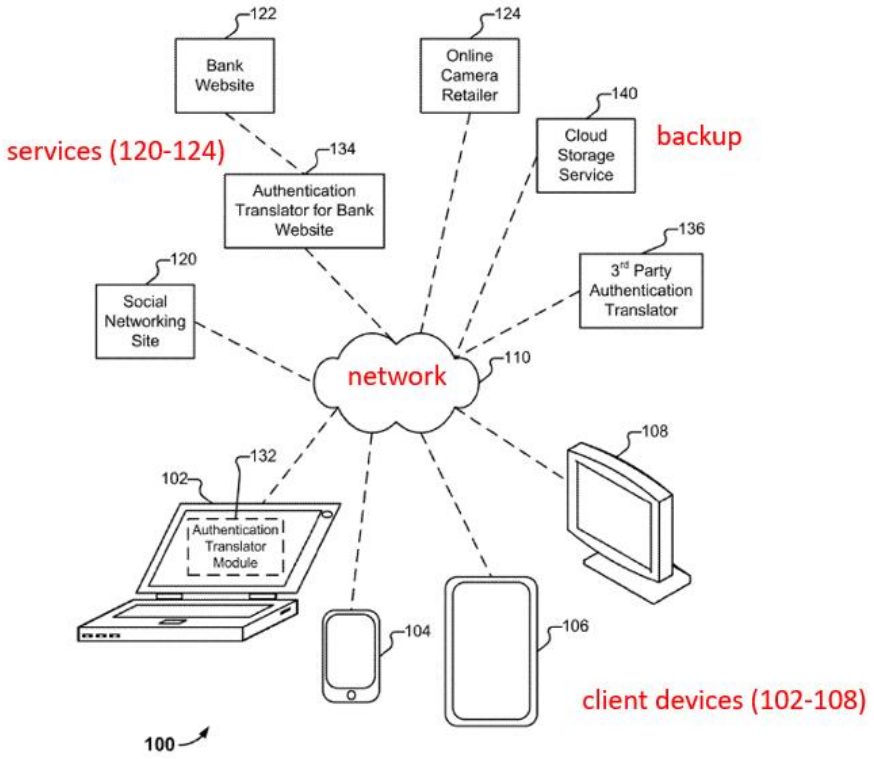
application is insufficient. In particular, in order for the earlier priority date to be applicable, the prior application must describe the claimed invention, and must do so in sufficient detail that one skilled in the art can clearly conclude that the inventor had possession of the claimed invention 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

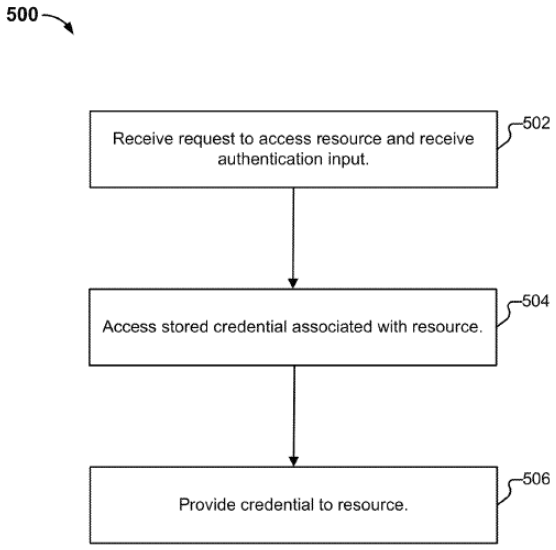
31. The '105 patent is directed to an environment that includes a client device, such as a notebook computer, smartphone, or tablet, which is connected via a network such as the Internet to a service such as a website. ('105 patent) APPL-1001, 2:62-3:14. FIG. 1 the '105 patent illustrates such an environment 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 Ke produces new data (called ciphertext C) that hides the original data, i.e., E(Ke,P) = C. A decryption function D associated with the given encryption function E takes the ciphertext and a decryption key Kd and produces the original plaintext, i.e., D(Kd,C) = P. The important part is that the plaintext P cannot feasibly be recovered from the ciphertext C without Kd[5], and therefore the encryption protects the underlying plaintext P from access by users who do not possess the decryption key Kd.

[5] Note that in many cases, Ke and Kd 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, other than the following:

A. "*restricted interface" (Claims 9-11 and 28-30)*

63. A "*restricted interface*" is an interface that limits accessibility. The accessibility may be limited through physical or software. As described above (*see* Section V.), the '105 patent issued on a CIP application that adds description beyond that appearing in the applications to which it claims priority. In particular, the '105 patent adds new disclosure that provides new examples of a "*restricted interface*" beyond the original disclosure of its priority applications. *See* APPL-1001, 11:30-24:39 ("Additional Embodiments"). Turning first to the original disclosure, the '105 patent (like the US 11,514,138, to which the '105 patent claims priority as a CIP, and its parent US 10,929,512) describes an example device including "a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader)," the specification refers to access limitations in the device in connection with an application programming interface (API). ('105 patent) APPL-

1001, 4:29-33 ("users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API"). Thus, a POSITA would understand *restricted interface* to at least include an API that limits accessibility to secure storage, a fingerprint sensor, or dedicated processor. In addition to this originally described form of *restricted interface*, the '105 patent adds examples including "dedicated physical connection from a processor permitted to access the secure storage," such as "a bus" or secure storage that is "integrated with the processor" such as "a SoC (System on a Chip)" as well as forms of "an API (Application Programming Interface)" having limited accessibility. ('105 patent) APPL-1001, 18:45-61.

64. I demonstrate in the following analysis that the prior art renders obvious a *restricted interface* to the extent it is given its plain and ordinary meaning, is an interface that limits accessibility, and/or includes configurations explicitly described in the '105 patent in hardware and API examples that limit accessibility to secure storage, a fingerprint sensor or a dedicated physical connection.

VIII. CLAIMS 1, 9-11, 14, 18, 28-30, 33 AND 35 ARE UNPATENTABLE

65. I have been asked to provide my opinion as to whether Claims 1, 9-11, 14, 18, 28-30, 33 and 35 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.

66. 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.

67. 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, 14, 18, 33, 35	§103(a) over Kesanupalli, Cheng and Kodama
#2	9-11, 28-30	§103(a) over Kesanupalli Cheng and Kodama in further view of Challener
#3	1, 9-11, 14, 18, 28-30, 33, 35	§103(a) over Jakobsson 351 and Kodama

68. 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, Kodama and Challener 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.

69. With respect to Ground #3, 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 Ground #3. I understand from Counsel that each of Jakobsson 351 and Kodama qualify as prior art with respect to this priority date of Dec. 15, 2020.

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

1. Summary of Kesanupalli

70. 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).

71. 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-

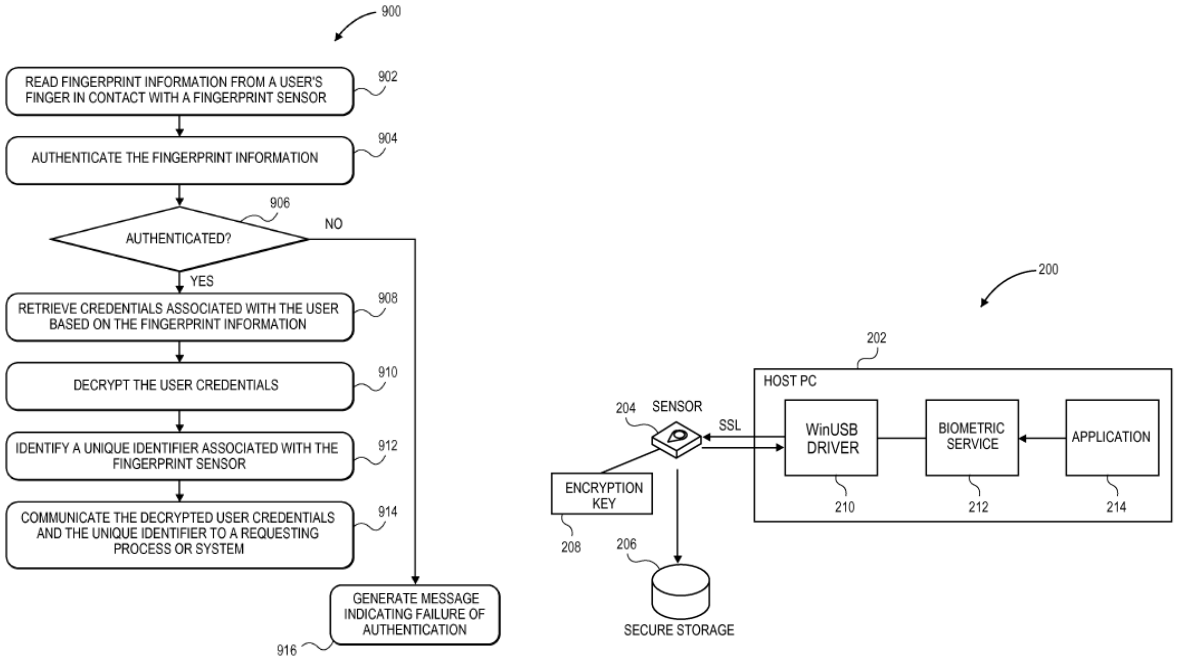
1006, 1:1-2:59-62. For example, based on a match between a fingerprint template stored for a particular user and fingerprint information read from a finger presented at a fingerprint reader, Kesanupalli's methods retrieve credentials associated with the user and communicate those credentials to an external system or process. (Kesanupalli) APPL-1006, FIGS. 8, 9.

72. 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.

73. 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.

74. 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

75. 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.

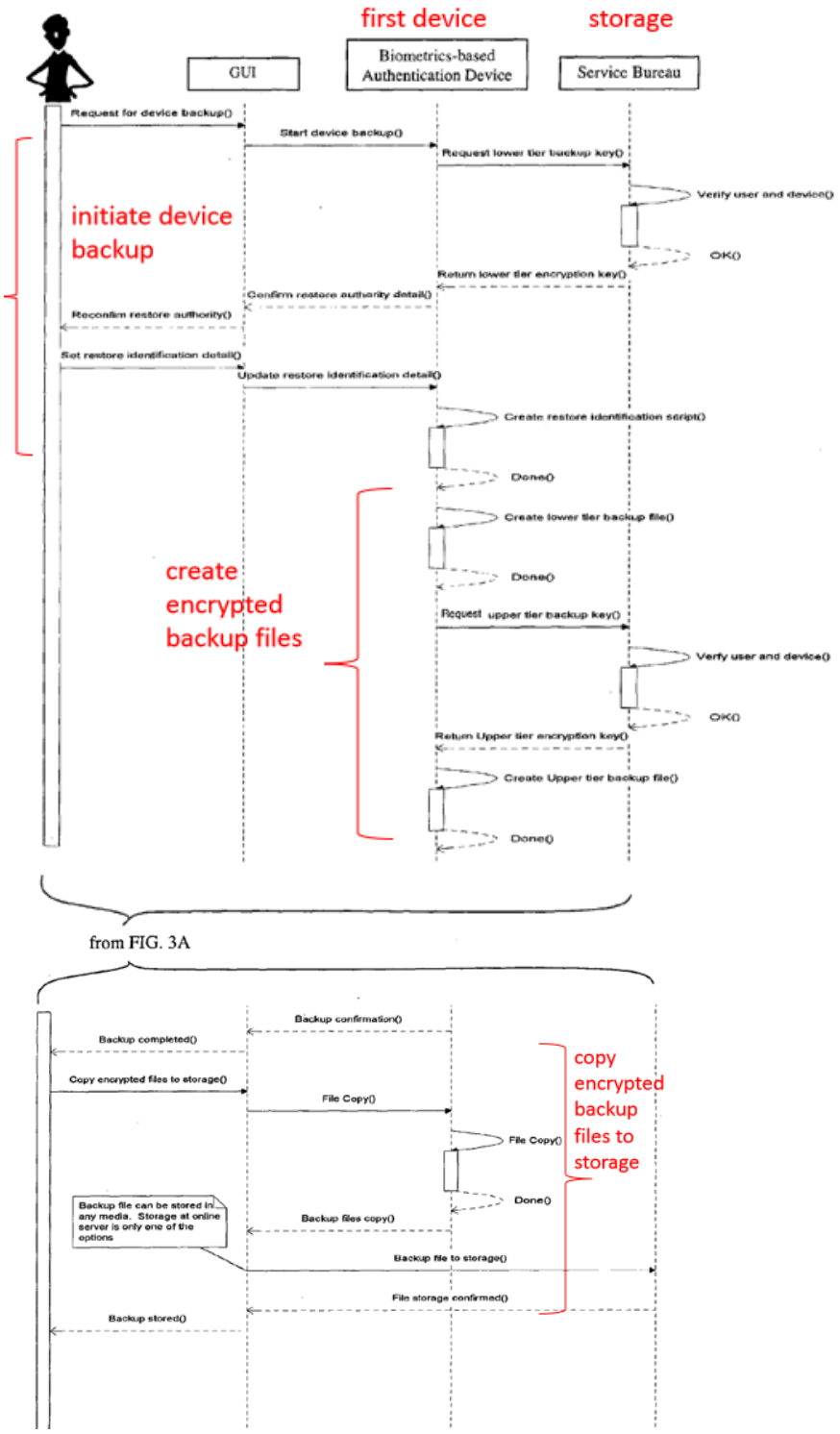
2. Summary of Cheng

76. 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).

77. 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].

78. Cheng performs a secure backup of this data to avoid costs of creating

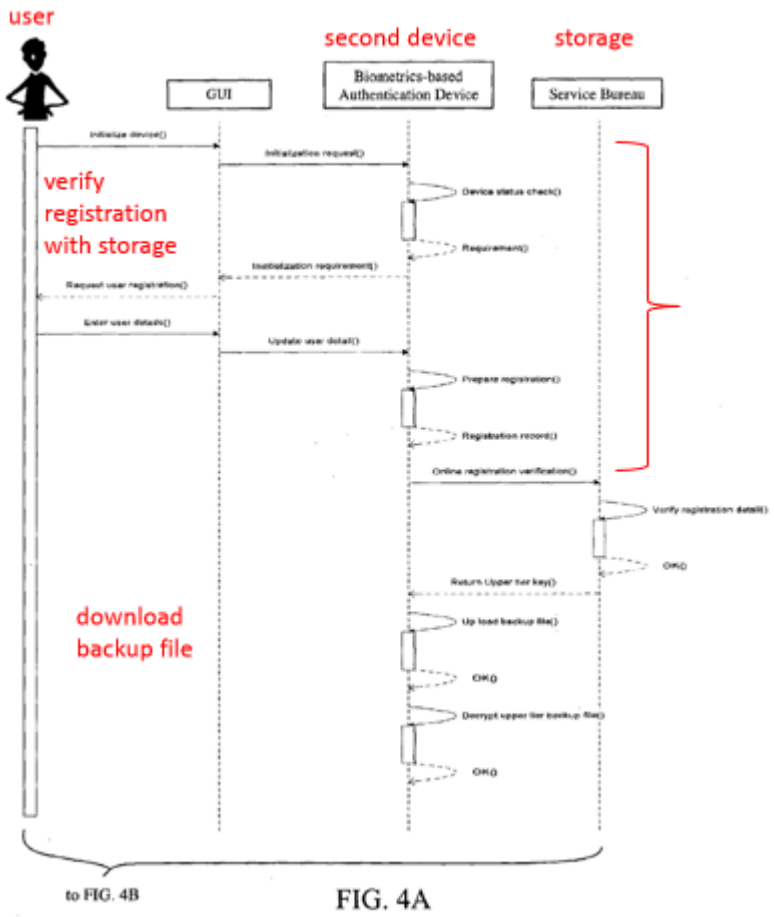
the data on new device from scratch should a first device containing the data be lost or stolen. *See* (Cheng) APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng's FIGS. 3A-3B where a backup of data of a first user's device is performed through secure communication between 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

79. 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

80. 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].

81. 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].

82. 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

83. 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.

84. 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.

85. 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].

86. 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 G0F6 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.

87. 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].

88. 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.

89. 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.

90. 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].

91. 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." APPL-1010, [0157]. See also, 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.

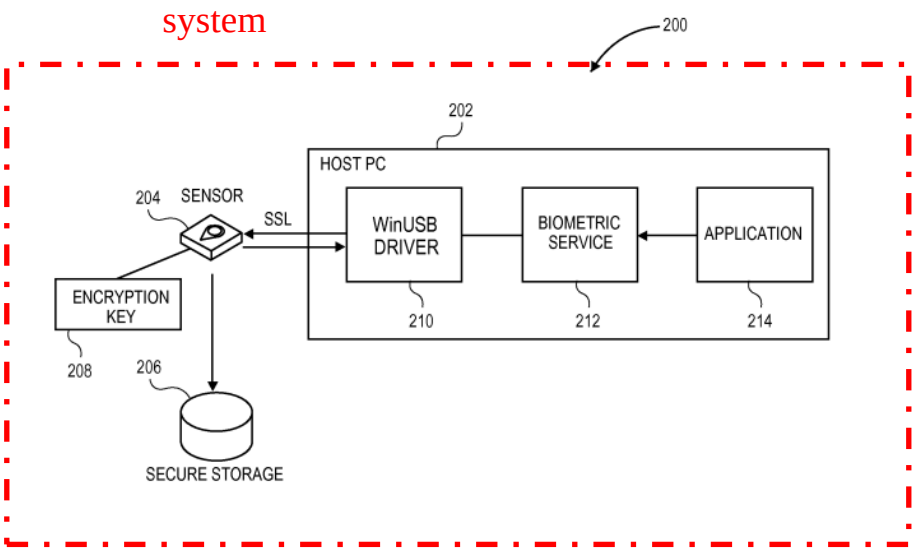
92. A POSITA would have had reasonable expectations of success in adding backup feature such as taught by Cheng as enhanced by Kodama in a biometric authentication system such as taught by Kesanupalli, as Cheng and Kodama are similarly directed to handling of personal information including biometric 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:*

93. Kesanupalli discloses *a system*.

94. 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.

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

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

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

97. 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.

98. 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*.

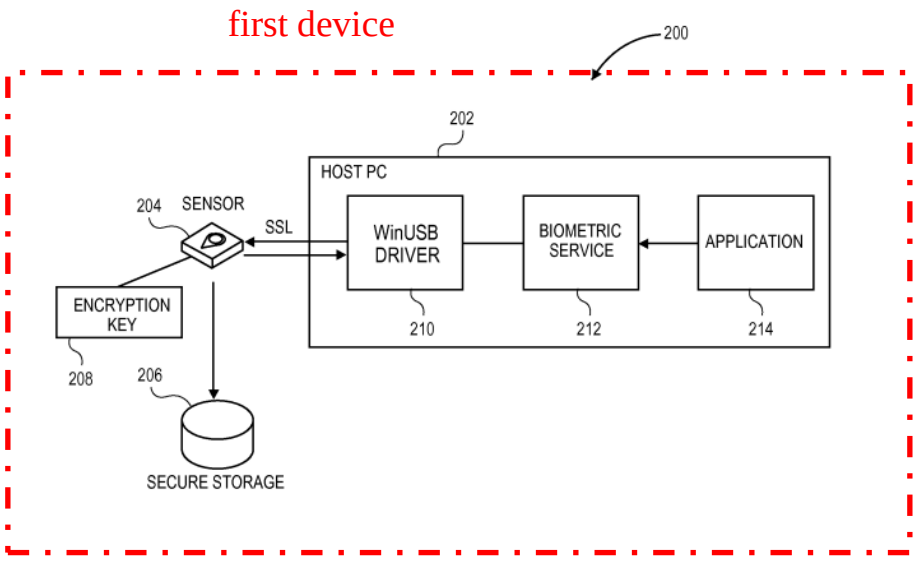
99. Thus, Kesanupalli discloses *one or more processors*.

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;*

100. 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*.

101. 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].

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



APPL-1006, FIG. 2, annotated

103. 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 webservers. APPL-1006, Abstract, 2:54-3:3, 4:3-11, 4:36-50, 6:11-49.

104. 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

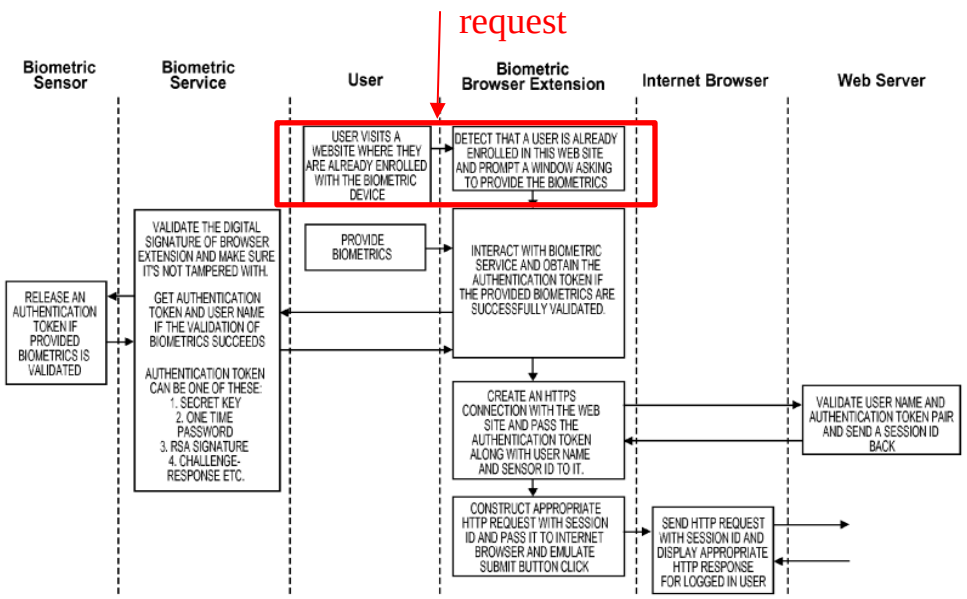
embodiments, the biometric sensor is physically attached (or manufactured into) a client device such as a computer, cellular phone, and so forth. which also includes the sensor 204." (Kesanupalli) APPL-1006, 2:48-50. *See also*, (Kesanupalli) APPL-1006, 3:46-51 ("In one embodiment the secure storage 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.")

105. 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

106. 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.

107. 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.

108. 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*,

109. 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*.

110. 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.

111. 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.")

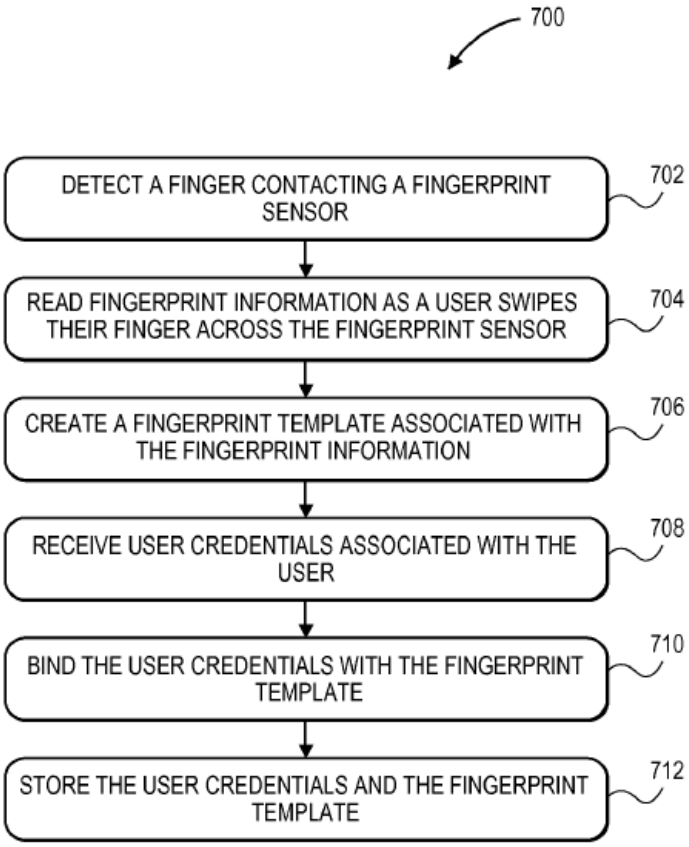


FIG. 7

112. 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.

113. 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.

114. 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

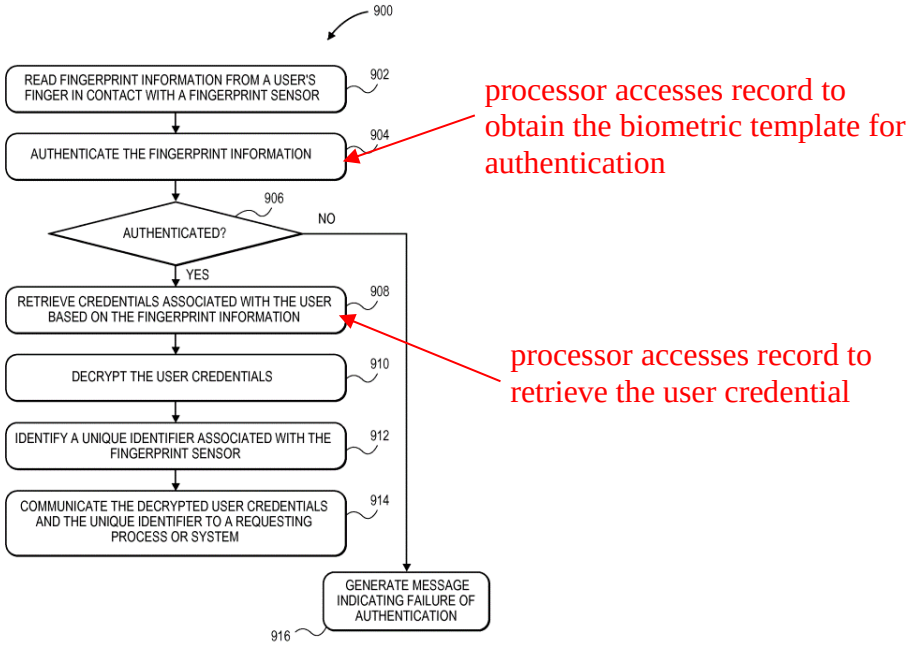
provide a collection of elements together.

115. 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

116. 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.

117. 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.

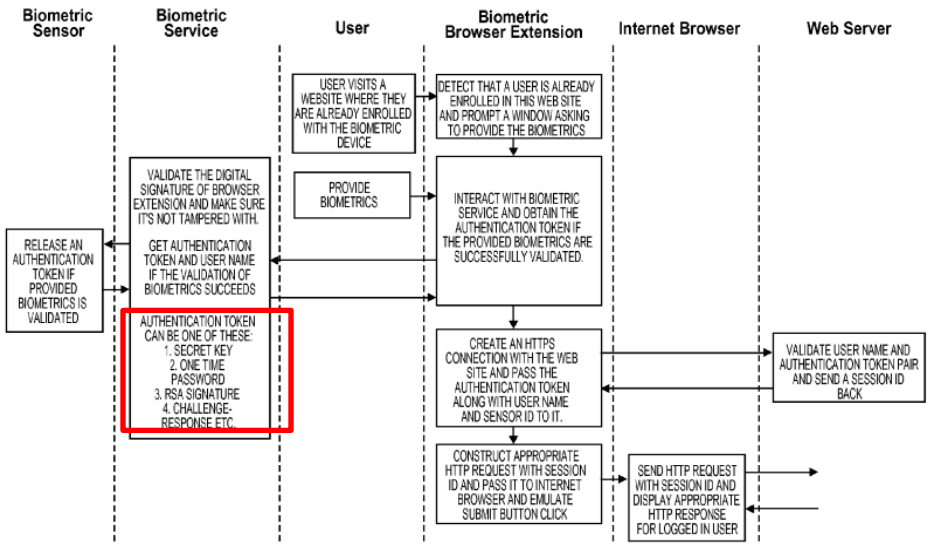
118. Thus, Kesanupalli discloses this element.

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

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

120. 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

121. Thus, Kesanupalli discloses this element.

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

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

123. 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.

124. 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;*

125. 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*.

126. 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.

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

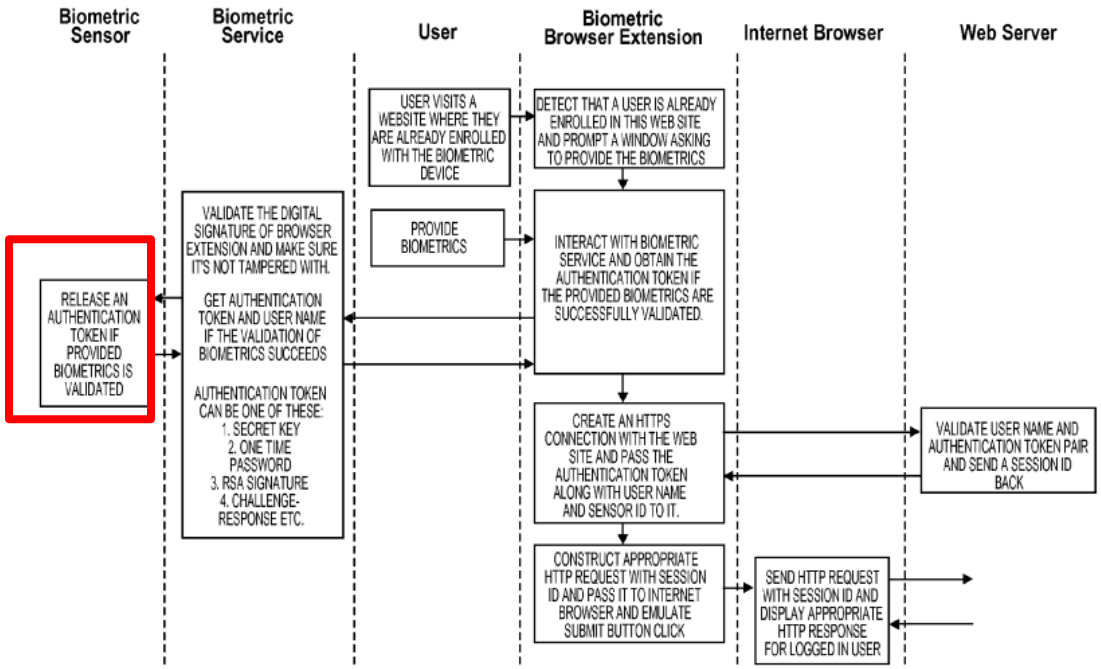
> The procedure then authenticates the fingerprint information (block 904). ... If the fingerprint information is authenticated, the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The procedure then decrypts the user credentials (910) ...

(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

128. 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;***

129. 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.

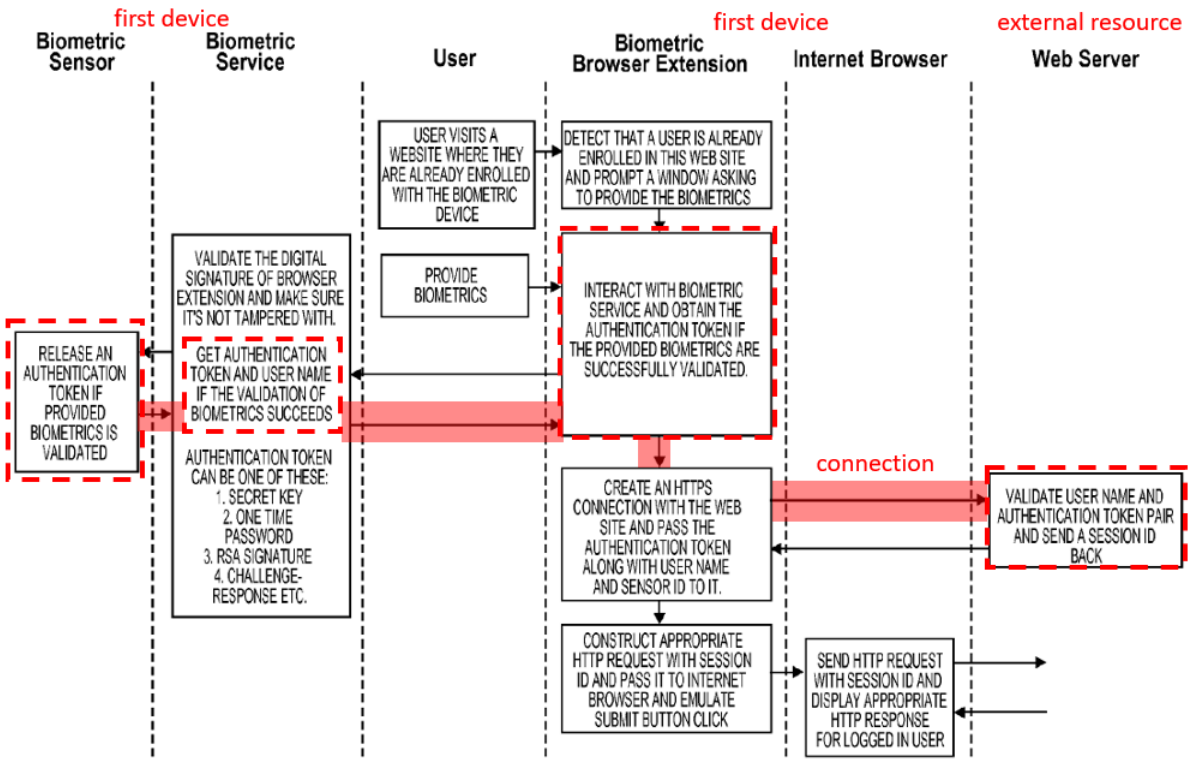
130. In particular, as discussed above in element [1.3a], the *record* (template and credential) is stored in the secure storage 206 of the first device. The credential is retrieved from the record in storage as Kesanupalli describes transferring the credential from the storage to a requesting resource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

131. 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

132. 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***

133. Kesanupalli discloses element [1.7].

134. 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.

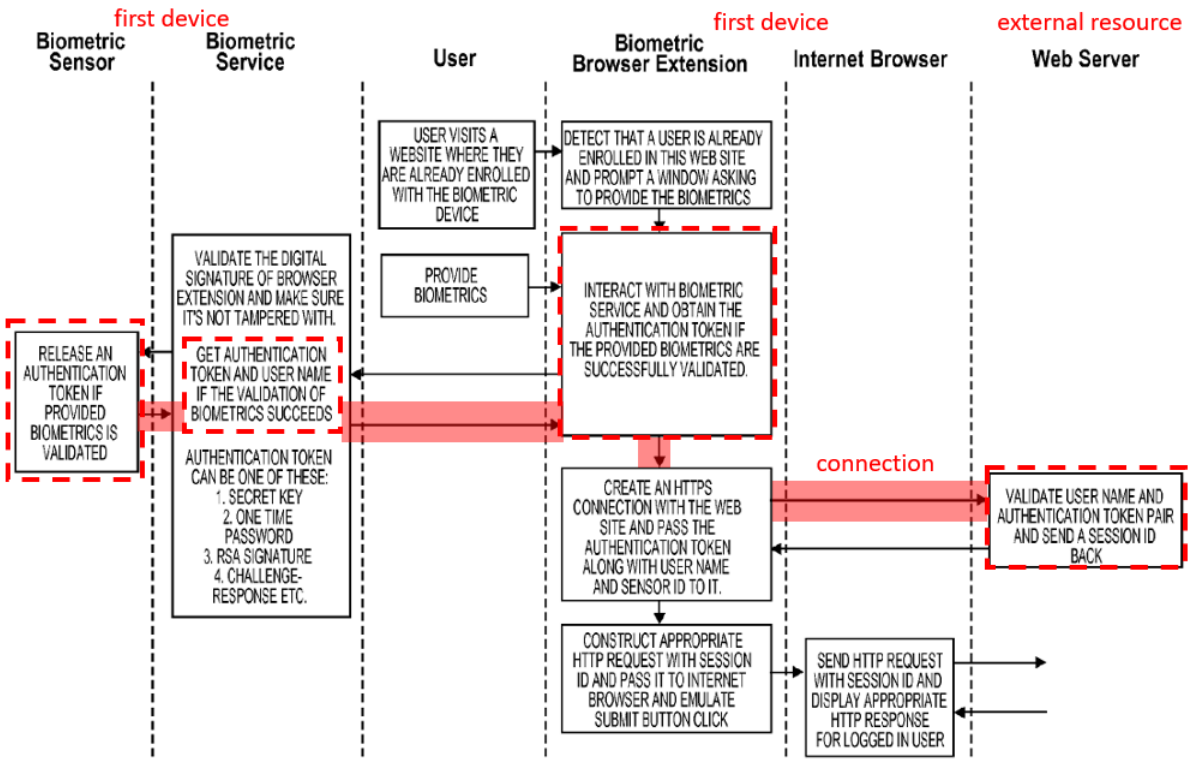
135. In Kesanupalli's device, the one or more processors *facilitate access*

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*.

136. 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.

137. 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.

138. 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.

139. 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.

140. 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*

141. 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*.

142. 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").

143. 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.

144. 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.

145. 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].

146. 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.

147. 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.

148. 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.

149. 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 is of the second device is the same as the first device.

150. 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.*

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

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

152. 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.")

153. 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.

154. Thus, Kesanupalli teaches this element.

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

6. Claim 14

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

156. Claim 1 is obvious over Kesanupalli, Cheng and Kodama, and

Kesanupalli discloses *the authentication input from the user is received using a biometric user input element*.

157. As illustrated above, Kesanupalli's authentication input is a biometric input of the user. A biometric input is received using a *biometric user input element* such as a fingerprint sensor.

> Particular examples discussed herein use fingerprint biometric information to authenticate one or more users. In other embodiments, any type of biometric information may be used instead of fingerprint information. Additionally, a particular embodiment may utilize multiple types of biometric information (e.g., fingerprints and voiceprints) to authenticate a user. Certain described embodiments refer to "swipe" style fingerprint sensors. However, alternate embodiments may include any type of fingerprint sensor, such as a "placement" sensor. ...

(Kesanupalli) APPL-1006, 2:39-53. *See also*, (Kesanupalli) APPL-1006 FIG. 2.

158. Therefore, Claim 14 is obvious in light of Kesanupalli, Cheng and Kodama.

7. Claims 18 and 33

159. 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] *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;*	[1.2]
[18.2] *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;*	[1.3a], [1.3b]
[18.3] *receiving authentication input from the user;*	[1.4]
[18.4] *determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;*	[1.5]
[18.5] *retrieving at least a portion of the credential information from the at least one record stored on the first device;*	[1.6]
[18.6] *facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output*	[1.7]

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

[18.0] ***A method, comprising:***

160. 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.

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

162. Dependent Claim 33 is substantively identical to Claim 14 discussed above, except that it depends from the method Claim 18. The combination of Kesanupalli, Cheng and Kodama renders obvious this claim for the same reasons discussed above with respect to Claim 18 and Claim 14.

8. Claim 35

163. The limitations of Claim 35, except the preamble, are substantively identical to limitations of Claim 1 already addressed above, as correlated in the table below:

Claim 35 Limitation	Corresponding Limitation of Claim 1 illustrating the limitation of Claim 18 is disclosed in Kesanupalli, Cheng, and/or Kodama
[35.1] *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;*	[1.2]
[35.2] *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;*	[1.3a], [1.3b]
[35.3] *receiving authentication input from the user;*	[1.4]
[35.4] *determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;*	[1.5]
[35.5] *retrieving at least a portion of the credential information from the at least one record stored on the first device;*	[1.6]
[35.6] *facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and*	[1.7]
[35.7] *based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.*	[1.8]

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

164. To the extent the preamble is limiting, Kesanupalli discloses it.

165. The citations to Kesanupalli in view of Cheng and Kodama above apply to a *system* as in Claim 1, and also to a *computer program product embodied in a non-transitory computer readable storage medium*. Kesanupalli discloses a *computer program product* can comprise instructions for the processes including those executed by its sensor 204 and a computing host (PC) 202 discussed above. *See* (Kesanupalli) APPL-1006, 9:58-10:12 ("configured to perform particular tasks according to the invention, by executing machine-readable software code that defines the particular tasks embodied by the invention."), 13:8-39.

166. Thus, Claim 35 is obvious over Kesanupalli, Cheng, and Kodama.

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

1. Summary of Challener

167. Challener "relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features." (Challener) APPL-1007, 1:7-9, 3:24-26. Challener illustrates a

system 10[10] (*e.g.*, computer or electronic device) with a system architecture suitable for securing data and functions of system 10 from unauthorized access and manipulation. (Challener) APPL-1007, 3:48-56. In particular, Challener describes system implementations in accord with a well-known Trusted Platform Module (TPM) specification promulgated by a standards organization, the Trusted Computing Group (TCG). *See* (Challener) APPL-1007, 3:54-56. As explained in Challener, in accord with the TPM specification, a standard chipset including a programmable microcontroller can be provided and used to store and secure information of the system that is desired to be protected.

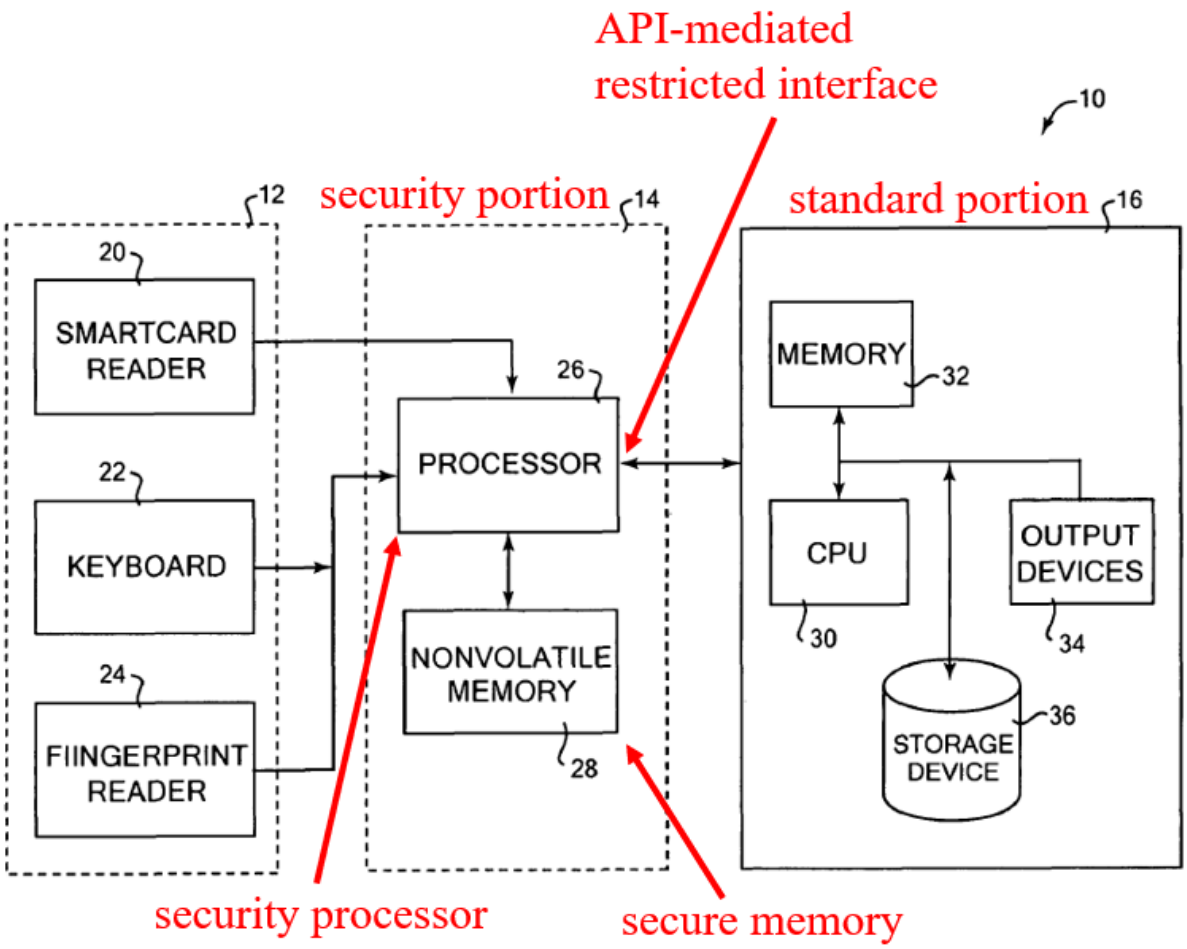
168. TPMs provide a platform for effective trusted computing features. (Challener) APPL-1007, 1:18-31. The security architecture (*i.e.*, the processor functions and the application program interface (API)) that runs on the microcontroller) can be referred to as a TPM. A TPM can offer a variety of features, including a random number generator, facilities for secure generation of

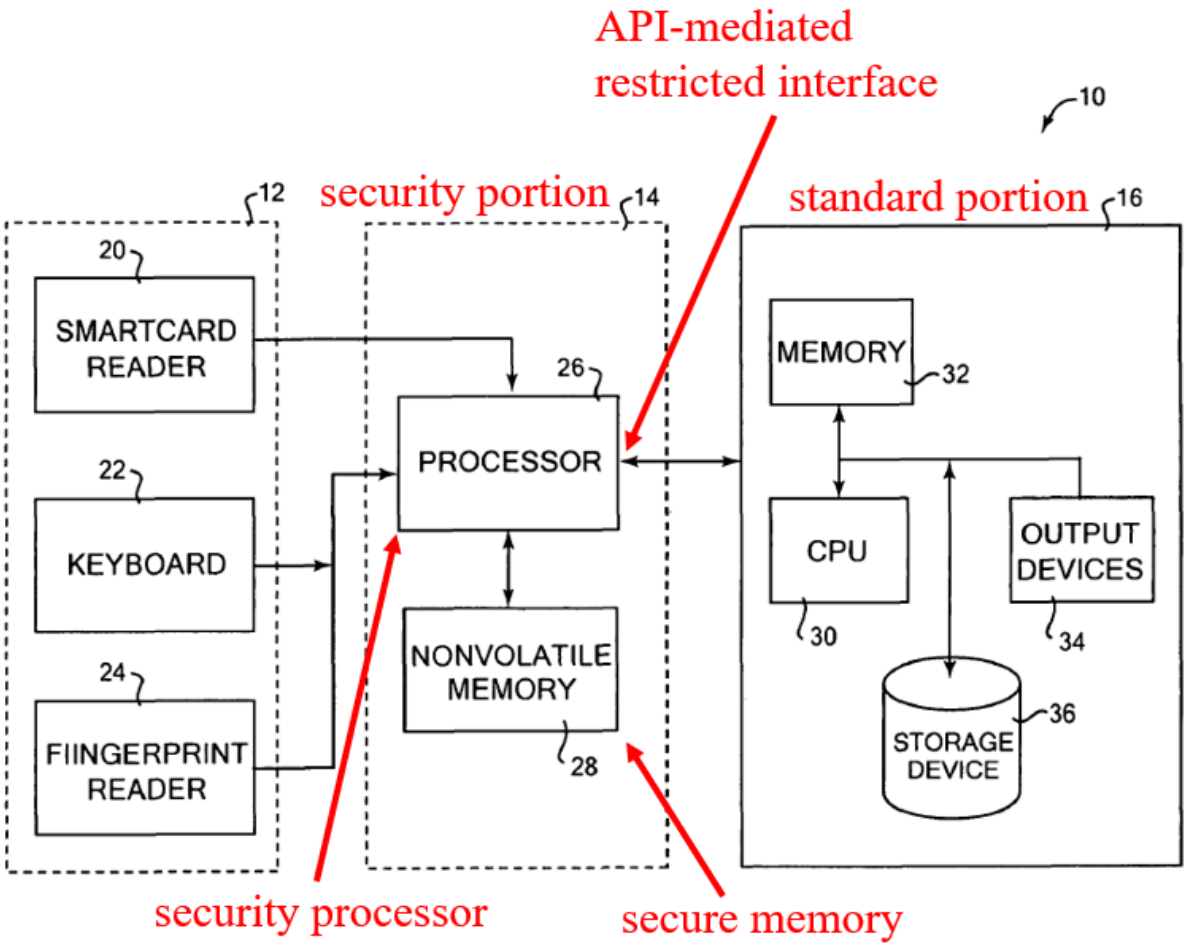
[10] "System 10 is a computer system having any of a variety of forms. For example, the computer system can be a mainframe computer, desktop computer, workstation, portable computer, or electronic device." (Challener) APPL-1007 3:37-51.

cryptographic keys, and abilities to limit the use of keys, e.g., to signing and verification, and/or encryption and decryption. (Challener) APPL-1007, 1:18-31. And as recognized by Challener, the TPM provides API-mediated interfaces. (Challener) APPL-1007, 1:25-27, 4:14-20. The TPM specification defines these API mediated interfaces as part of the TPM.[11] One example of such the API-mediated interface in a TPM architecture is "The SEAL operation allows software to explicitly state the future "trusted" configuration that the platform must be in for the secret to be revealed. [...] If the UNSEAL operation succeeds, proof of the platform configuration that was in effect when the SEAL operation was performed is returned to the caller, as well as the secret data."[12] In other words, a component can ONLY access the TPM if it is in a "trusted" (i.e., restricted) configuration.

[11] See APPL-1017 https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf.

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


API-mediated
restricted interface
10
12
security portion
14
standard portion
16
20
SMARTCARD
READER
22
KEYBOARD
24
FIINGERPRINT
READER
26
PROCESSOR
NONVOLATILE
MEMORY
28
MEMORY
32
CPU
30
OUTPUT
DEVICES
34
STORAGE
DEVICE
36
security processor
secure memory



(Challener) APPL-1007, FIG. 1, annotated

169. Challener provides an implementation framework for secure systems, which may be TPM-based, and which includes an input portion 12, a security portion 14, and a standard portion 16. *See* (Challener) APPL-1007, 3:46-57. Security portion 14 is used to secure data and applications of the system for access and use only by authorized users through a dedicated security processor 26 and a memory 28. (Challener) APPL-1007, 4:9-65. The memory 28 is connected to the processor 26 and "is a secure memory which cannot be easily tampered with to

read its data contents" and can be on the same chip or package as the memory 28. *Id*. The standard portion 16 is connected to the security processor 26 (via its APLI-mediated interfaces) and includes a microprocessor 30 that controls general operation of the system including input/output functions. (Challener) APPL-1007, 5:15-25.

2. Reasons to Combine Kesanupalli in view of Cheng and Kodama and Challener

170. A POSITA would have been motivated to apply Challener's teachings of a TPM-type security architecture with API-mediated interfaces between secure portions and less-secure portions of a system in implementations of Kesanupalli's methods for secure user authentication using biometric information with Cheng and Kodama's backup of data to a second device teachings. The combination would have produced the obvious, beneficial, and predictable results of a standardized and widely-deployed security architecture for implementation of Kesanupalli and Cheng/Kodama's techniques.

171. **First**, Challener, Kesanupalli, Cheng and Kodama and the '105 patent are analogous art and are all in the same field of endeavor–namely, information security, and more particularly, security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. (Challener) APPL-1007, 1:7-9 ("The present invention relates to securely protecting computer data, and more particularly to security processors provided in computer systems to

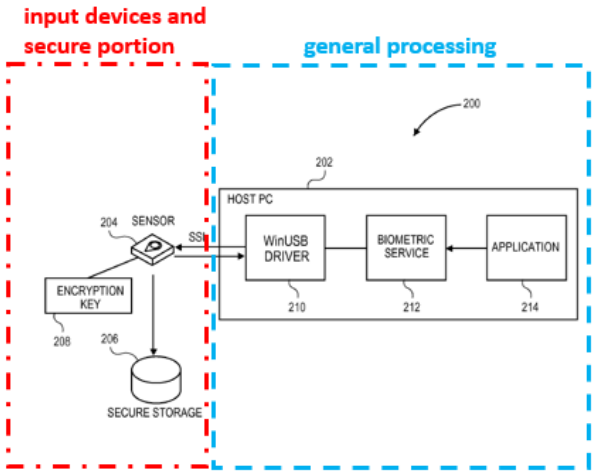
implement security features."), 3:52:56 ("Trusted Platform Module (TPM) … for securing data and functions of the system [] from unauthorized access and manipulation."); *see also supra* VIII.A.3 (reasons to combine Kesanupalli and Cheng and Kodama). Moreover, Challener bears the very the IPC subclass—CPC/IPC G0F6 21 as discussed above relative to Kesanupalli, Cheng/Kodama and the '105 patent. (Challener) APPL-1007, (51). *See also*, my claim construction discussion above.

172. Second, a POSITA would have been motivated to apply Challener's teachings of a standards-based TPM architecture as an implementation framework for Kesanupalli's biometric security techniques given the support that a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided. (Challener) APPL-1007, 1:18-31 (summarizing typical TPM functions and APIs). Indeed, Challener's particular description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data, e.g., "secure hash values and … keys," *and* fingerprint reader 24 behind a security processor 26 that "implements the particular security features and functions (e.g., API functions, algorithms)" in a system that includes secure and non-secure portions. (Challener) APPL-1007, 4:57-5:9, 3:67-4:23. These are precisely the security architecture features that a POSITA having Kesanupalli before her would be motivated to

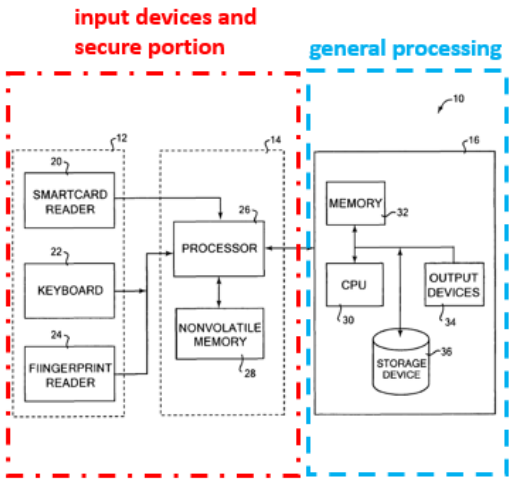
implement in a standards-based security architecture that would engender trust amongst users and customers (at least for the compatibility and reliability of the platform).[13] A POSITA would have had reasonable expectations of success in implementing Kesanupalli's a biometric authentication techniques and in applying Cheng and Kodama's backup given that Challener's architecture applies TPM techniques, which were well-known, standard and widely-deployed in the industry. *See* (Challener) APPL-1007, 1:18-31; *see also* Section VI. Technology Background. In contrast, Kesanupalli's architecture, which while it shares features with a TPM-based system is, as Challener states one of many different techniques used to secure information and does not enjoy the confidence of the end-to-end systems implemented under the known TPM specification. Further, Kesanupalli itself suggests the use of specialized processors. (Kesanupalli) APPL-1006, 9:64-10:1. TPM is just such a specialized processor

173. Additionally, Challener's description of TPM architecture would have been attractive because of the correspondence of general and secure processor portions, secure storage, and a fingerprint reader described in Challener's TPM based implementation with functional blocks described in Kesanupalli.

[13] *See*, *e.g.*, APPL-1016, https://www.iso.org/standard/50970.html



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Note that while the WinUSB driver of Kesanupalli (108) performs security functions such as encrypting template and credential information, it is fully compatible with the suggestion of Challener's TPM. Indeed, a POSITA would be highly motivated to move the security functions performed by the WinUSB driver in Kesanupalli into the TPM because it would provide stronger security by isolating the keys and operations away from the general-purpose processor—and therein ensure protection against local operating system compromises from viruses or other malware. See, (Kesanupalli), APPL-1006 5:66-6:4, 6:28-31.

174. Finally, a POSITA would have had reasonable expectations of success in implementing to Kesanupalli's biometric authentication techniques in view of Cheng and Kodama using Challener's TPM-based architecture techniques, as TPM techniques were well-known, standard and widely-deployed in the

industry. *See* (Challener) APPL-1007, 1:18-31, *see* Section VI.E. In contrast, Kesanupalli's architecture, which while it shares features with a TPM-based system is as Challener states one of many different techniques used to secure information and does not enjoy the confidence of the end-to-end systems implemented under the known TPM specification. Further, Kesanupalli itself suggests the user of specialized processors. (Kesanupalli) APPL-1006, 9:64-10:1. TPM is just such a specialized processor.

3. Claim 9

[9.0] ***The system of claim 1,***

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

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

175. First, Kesanupalli discloses *the at least one record stored on the first device is stored in a secure storage*. As discussed above, the storage is provided by Kesanupalli's "secure storage 206." *See* (Kesanupalli) APPL-1006, FIG. 2, 6:45-49 ("User credentials and other information may be stored within biometric sensor 204, in a secure storage 206, or any other storage mechanism.")

176. A *secure storage* is one that is protected from unauthorized access. By describing its storage as "secure storage," a POSITA would understand Kesanupalli to be providing a secure storage area that is protected from

unauthorized access. Additionally, as illustrated by FIG. 2, access to the secure storage 206 is controlled by the sensor 204. And access to other applications such as the application 214 is not directly available, except as accessed by the sensor 204. Further, Kesanupalli describes a secure storage as the data, the credential, remains in location and is not released unless a match authenticating a user is performed. Therefore, the credential in the secure storage cannot be accessed unless authorized by the processor executing the functions of the sensor 204. The secure storage maintains its protected character when implemented in Challener's secure architecture. (Challener) APPL-1007, FIG. 1, 4:56-65 describing element memory 28 in security portion 14 connected to the processor 26, "memory 28 is a secure memory which cannot be easily tampered width to read its data contents. [and] can be included on the same integrated circuit chip, or package, or the processor 26."

177. As to element [9.0b], as discussed above at element [1.3], the one or more processors is configured to access at least one record stored in storage, secure storage 206 of Kesanupalli. Kesanupalli and Challener together teach this interface is a restricted interface. As background, an interface is a software and/or hardware structure that enables two components in a computer system to exchange information. Interfaces enable components to interact with each other while isolating internal algorithms and structures from external logic. When practiced in

software, documented interfaces are generally referred to as APIs (application programmer interfaces). In computer systems, processors access coupled components such as storage using defined (and often standardized) interfaces. These interfaces act as protocols or "rules of the road" for data transfer between components. Such rules are necessary to ensure that different processors and storage systems can be used (or replaced) within the computer system without affecting other component logic with which they interact over the interface. Such abstraction and internal logic isolation is at the heart of modern computing systems and is a driving force behind the scalability and flexibility of their design.

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

functions of the processor, just like the secure storage 206 of Kesanupalli. (Challener) APPL-1007, 5:5-7.

179. In Kesanupalli implemented on Challener's architecture, the security processor (e.g., sensor 204) is configured to access the at least one record stored on the secure storage using a *restricted interface*, as that term is explained in the '105 patent. Kesanupalli suggests that its secure storage 206 is "within the biometric sensor 204." APPL-1006, 6:45-47. Challener further illustrates that secure storage is not merely formed on a same device, but "included on the same integrated circuit chip." (Challener) APPL-1007, 4:63-65. This is precisely one of the example *restricted interfaces* of the '105 patent. ('105 patent) APPL-1001, 18:53-55. A POSITA would also recognize that Challener teaches that the memory may be integrated with the processor, which is another example of a *restricted interface* in the '105 patent. (Challener) APPL-1007, 9:49-51 ("the selected application is loaded into memory of processor 26 (such as non-volatile memory 28 or other available memory)").

180. As explained above, "*restricted interface*" is an interface that limits accessibility. Based on the '105 patent's description a "*restricted interface*" would be understood to at least include an API that limits accessibility to a secure storage, a fingerprint sensor, or dedicated processor. S*ee* Section VII. In particular, Kesanupalli (implemented using Challener's TPM framework for secure systems),

provides communication between the security portion (14), including processor (26) and its secure storage (28), and the standard portion (16) occurs through a *restricted interface* as detailed below.

181. TPM-based implementations, including Challener's TPM-based implementation, are widely recognized examples of a security architecture that provides a *restricted interface* in the form of an access limiting API to restrict access to the TPM (secure processor) by programs running on a general processor in a standard (non-secure) portion of a system to the security-related operations and data, such as key and credential management, secure storage, encryption, decryption and digital signatures, that are provided or maintained in a secure portion of the system. Section VI.E. *See also*, (Challener) APPL-1007, 4:3-15 discussing controlling "access."

182. Challener discloses an interface (an API) that used in the communication of the general processor and the secure storage in its TPM-based architecture. This is because access to the memory must be via the secure processor (26) of Challener, which implements a security architecture that includes API functions used in its communication with other components – including the general processor 30. APPL-1007, 4:9-24 ("The processor 26 typically implements a 'security architecture' which, as used herein, refers to the particular security features and functions (e.g. API functions, algorithms) implemented for

the system 10 as determined by a security architecture application loaded on the processor 26."), FIG. 1. An API is an interface with a distinct function of defining how two components, here the software executing on processor 26 and the software executing on general processor 30 communicate with one another as discussed above in Section VI.E. And a TPM-based API, such as provided by Challener's processor 26, provides restrictions by the way of a set of rules or restrictions that are defined by the TPM standard for access to the security portion 16 of the system.

183. Thus, implementing Kesanupalli (as modified by Cheng/Kodama) using the architecture of Challener provides communication between the general processor (PC 202) and security processor (sensor 204) via a *restricted interface* (e.g., via an API of the TPM security architecture of the security processor executing the processor functions of sensor 204). This is merely a predictable use of a known element according to its established function in the TPM architecture. Thus, Claim 9 is also obvious over Kesanupalli, Cheng, Kodama in view of Challener.

4. Claim 10

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

184. As discussed above with respect to Claim 9, a POSITA would recognize that Kesanupalli implemented on Challener's TPM includes a dedicated

physical connection between the one or more processors and the secure storage 206. The secure memory is accessible **only** via the secure processor and thus, has a dedicated connection to the memory. See, (Kesanupalli) APPL-1006, (Challener) FIG. 2; APPL-1007, FIG. 1. The memory is physically "on-chip" or integrated with the processor, thus is a dedicated physical connection such as a dedicated chip level conductive interconnect between the secure processor circuitry and its associated memory. (Challener) APPL-1007, 4:60-65, 9:49-51. Therefore, a POSITA would recognize a restricted interface of a dedicated physical connection would have been obvious in light of Challener's teachings. Thus, claim 10 is obvious over Kesanupalli, Cheng, Kodama, and Challener.

5. Claim 11

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

185. As discussed above with respect to Claim 9, a POSITA would recognize that the restricted interface of Kesanupalli implemented on Challener's TPM architecture has a restricted interface between the one or more processors and the secure storage 206 as it includes an application programming interface.

186. Thus, Claim 11 is also obvious over Kesanupalli, Cheng, Kodama in view of Challener.

6. Claims 28-30

187. Dependent claims 28, 29 and 30 are substantively identical limitations

to claims 9-11 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 9-11 and 18.

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

1. Jakobsson 351 and Kodama

188. 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

189. 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.

190. 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).

191. 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." 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.

192. 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*:

193. 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.

194. Thus, Jakobsson 351 discloses this element.

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

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

196. 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*;

197. 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.

198. 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,***

199. 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.

200. Thus, Jakobsson 351 discloses this element.

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

201. 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.

202. Thus, Jakobsson 351 discloses this element.

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

203. 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.

204. 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*;

205. 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.

206. 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*****;**

207. 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.

208. 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***

209. 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.

210. 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*

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

212. 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.

213. 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*.

214. 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).

215. 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.

216. 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]. 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.

217. 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.***

218. 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.

219. Thus, Jakobsson 351 discloses this element.

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

4. Claim 9

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

221. Jakobsson 351 continues to describe its system includes "a secure storage ... wherein the record is stored in the insecure storage, and wherein obtaining access to the record comprises loading the record to the secure storage."

(Jakobsson 351) APPL-1011, 11:57-56.

222. Jakobsson 351 continues to describe its processors of the system are configured to access the at least one record stored on the secure storage using a restricted interface.

> One example of a device with secure storage is illustrated in FIG. 3. In the example shown, a mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader). Users (and applications) can read from and write to the insecure storage area. However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API.

(Jakobsson 351) APPL-1011, 3:54-63. Thus, Claim 9 is obvious over Jakobsson 351 and Kodama.

5. Claim 10

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

223. FIG. 3 of Jakobsson illustrates "secure storage 306 attached to a dedicated processor 308." APPL-1011, 4:7-8. A POSITA would have found it obvious to "attach" the secure storage to its dedicated processor using a *dedicated physical connection*. This is because a dedicated processor is the only way to

access the secure storage, therefore the dedicated physical connection is an obvious choice in implementing Jakobsson '351's design. APPL-1011, 3:54-63 including "processor can only communicate with the dedicated processor/sensor via a restricted API." Thus, claims 9 and 10 are obvious over Jakobsson '351 and Kodama.

6. Claim 11

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

224. Jakobsson 351 describes:

> One example of a device with secure storage is illustrated in FIG. 3. In the example shown, a mobile phone 300 includes a large and insecure storage 302 attached to a fast processor 304, and a smaller but secure storage 306 attached to a dedicated processor 308 and a sensor 310 (e.g., a camera or a fingerprint reader). Users (and applications) can read from and write to the insecure storage area. However, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API.

(Jakobsson 351) APPL-1011, 3:54-63.

225. Thus, Claim 11 is obvious over Jakobsson 351 and Kodama.

7. Claim 14

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

226. Jakobsson 351 continues to describe its system includes "a biometric input component," would provide "a biometric input..." (Jakobsson 351) APPL-1011, 11:22-26, 45-50.

227. Therefore, Claim 14 is obvious in light of Jakobsson 351 and Kodama.

8. Claims 18, 28-30, and 33

228. 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] *A method, comprising*:	(Jakobsson 351) APPL-1011, 12:21	
[18.1] *receiving, at a first device, a request to access a resource external to*	(Jakobsson 351) APPL-	[1.2]

the first device, wherein the resource external to the first device is associated with a user;	1011, 12:22 - 25	
[18.2] *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;*	(Jakobsson 351) APPL-1011, 12:26-39, 56-58	[1.3]
[18.3] *receiving authentication input from the user;*	(Jakobsson 351) APPL-1011, 12:22 - 25	[1.4]
[18.4] *determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;*	(Jakobsson 351) APPL-1011, 12:26-30	[1.5]
[18.5] *retrieving at least a portion of the credential information from the at least one record stored on the first device;*	(Jakobsson 351) APPL-1011, 12:31-39	[1.6]
[18.6] *facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and*	(Jakobsson 351) APPL-1011, 12:40-53	[1.7]

[18.7a] *based at least in part on the first device being a same brand as a second device,* [18.7b] *initiating a backup, to the second device, of at least a portion of the at least one record.*	As to [18.7b], (Jakobsson 351) APPL-1011, 14:16-22	[1.8]

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

230. Dependent Claims 28-30 and 33 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.

Claim	Additional Jakobsson 351 disclosure	Corresponding Claim Analysis above
[28]	(Jakobsson 351) APPL-1011, 13:17-23	[9]
[29]		[10]
[30]		[11]
[33]	(Jakobsson 351) APPL-1011, 12:65-13:2	[14]

9. Claim 35

231. The limitations of Claim 35, except the preamble, are substantively identical to limitations of Claim 1 already addressed above, as correlated in the table below:

Claim 35 Limitation	Corresponding Claim Limitation

[35.1] *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;*	[1.2]
[35.2] *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;*	[1.3a], [1.3b]
[35.3] *receiving authentication input from the user;*	[1.4]
[35.4] *determining that the authentication input from the user matches the authentication information associated with the user included in the at least one record stored on the first device;*	[1.5]
[35.5] *retrieving at least a portion of the credential information from the at least one record stored on the first device;*	[1.6]
[35.6] *facilitating access of the user to the external resource at least in part by transmitting, on behalf of the user, from the first device, output based at least in part on the at least portion of the credential information retrieved from the at least one record, wherein the user of the first device is granted access to the external resource based at least in part on the output transmitted from the first device on behalf of the user; and*	[1.7]
[35.7] *based at least in part on the first device being a same brand as a second device, initiating a backup, to the second device, of at least a portion of the at least one record.*	[1.8]

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

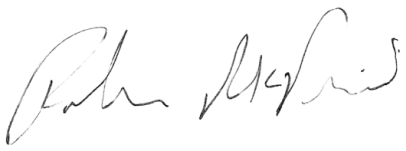
232. Jakobsson 351 states that is invention can be implemented by a

computer program product embodied in a non-transitory computer readable storage medium and comprising computer instructions for aspects cited in the analysis of the system discussed above. *See* Jakobsson 251, 1:57-2:7.

233. Thus, Claim 35 is obvious over Jakobsson 351 and Kodama.

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 18, 2024