

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

IPR2023-00334
U.S. Patent No. 11,514,138

**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	9
III.	Level of Ordinary Skill in the Art	12
IV.	Relevant Legal Standards	14
V.	Overview of the '138 Patent.....	16
VI.	Technology Background.....	21
	A. AUTHENTICATION.....	21
	B. CREDENTIALS AND CREDENTIAL MANAGEMENT.....	23
	C. CRYPTOGRAPHY	26
	D. CRYPTOGRAPHY IN WEB TRANSACTIONS.....	27
	E. TRUSTED PLATFORM MODULES	28
VII.	Claim Construction.....	30
	A. “processor”	31
	B. “restricted interface” (Claims 11, 23)	31
VIII.	Claims 1-3, 5, 7-8, 10-15, 17, 19, and 22-25 are Unpatentable	33
	A. Ground 1: Claims 1-3, 7-8, 12-15, 19, and 24-25 are obvious under 35 U.S.C. § 103 over Kesanupalli and Brown.....	35
	1. Summary of Kesanupalli	35
	2. Summary of Brown	38
	3. Reasons to Combine Kesanupalli and Brown.....	40
	4. Claim 1	45
	a) [1.0] A device, comprising:	45

- b) [1.1] *a processor on the device; 47*
- c) [1.2] *a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, ...51*
- d) [1.3] *wherein the processor on the device is configured to: based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device; 56*
- e) [1.4] *wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key; 64*
- f) [1.5A] *in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, ...66*
- g) [1.5B] *wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented; 71*
- h) [1.6] *establish a connection with the external resource; 73*
- i) [1.7] *facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and 76*
- j) [1.8] *facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and 80*

k)	[1.9] <i>a memory coupled to the processor and configured to provide the processor with instructions.</i>	84
5.	Claim 2	85
6.	Claim 3	86
7.	Claim 7	87
8.	Claim 8	89
9.	Claim 12	91
10.	Claims 13– 15, 19, and 24.....	92
11.	Claim 25	95
B.	Ground 2: Claims 10 and 22 are obvious under 35 U.S.C. § 103 over Kesanupalli in view of Brown and in further view of Cheng.....	98
1.	<i>Summary of Cheng</i>	98
2.	<i>Reasons to Combine Kesanupalli, Brown and Cheng</i>	101
3.	<i>Claim 10</i>	106
4.	<i>Claim 22</i>	108
C.	Ground 3: Claims 11 and 23 are obvious under 35 U.S.C. § 103 over Kesanupalli in view of Brown and in further view of Challenger.	108
1.	<i>Summary of Challenger</i>	108
2.	<i>Reasons to Combine Kesanupalli, Brown and Challenger</i>	112
3.	<i>Claim 11</i>	115
4.	<i>Claim 23</i>	119
D.	Ground 4: Claims 5 and 17 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Headley.....	120

1.	<i>Headley</i>	120
2.	<i>Reasons to Combine Kesanupalli, Brown and Headley</i>	121
3.	<i>Claim 5</i>	123
4.	<i>Claim 17</i>	124
IX.	Conclusion	125

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. 11,514,138 (“’138 patent”) concerning whether the ’138 patent is unpatentable over certain prior art. This declaration is a statement of my opinions on issues relating to the patentability of Claims 1, 3, 5, 7-8, 10-15, 17, 19, and 22-25 (“the Challenged Claims”) of the ’138 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 ’138 patent:

a) the ’138 patent, APPL-1001;

- b) the prosecution history of the '138 patent (“’138 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) U.S. Patent No 9,652,629 to Brown et al. (“Brown”), APPL-
1009; and
- g) U.S. Patent No. 8,185,646 to Headley (“Headley”), APPL-
1010.

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 including:

APPL-1012	Patrick McDaniel, <i>Authentication</i> , Handbook of Computer Networks, Volume 3, Part 2, pp. 570-580, John Wiley and Sons, 2008. Ed. Hossein Bidgoli
APPL-1013	IBM Introducing Fingerprint Reader Into Laptop. Jack Germain. 2004 at https://www.technewsworld.com/story/ibm-introducing-fingerprint-reader-into-laptop-37017.html (retrieved Dec. 12, 2023)
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 (retrieved Dec. 12, 2023)
APPL-1016	ISO/IEC 11889-1:2009 Information technology Trusted Platform Module Part 1: Overview at https://www.iso.org/standard/50970.html (retrieved Dec. 12, 2023)
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 (retrieved Dec. 12, 2023)
APPL-1018	Introduction to Programmable Systems on a Chip, Bob Zeidman, 07.27.2005 at https://www.eetimes.com/introduction-to-programmable-systems-on-a-chip/ (retrieved Dec. 12, 2023)
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/ (retrieved Dec. 12, 2023)
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 '138 patent was filed September 21, 2020 and claims priority through various continuations to provisional applications filed January 17, 2012 and December 9, 2011. My analysis reflects the views of a person of ordinary skill in the art ("POSITA") in the field of the '138 patent as of December 9, 2011.

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 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 earliest proper priority date of the '138 patent (*i.e.*, December 9, 2011). Unless otherwise stated, when I provide my understanding and analysis below, it is

consistent with the level of a POSITA prior to the earliest alleged priority date of the '138 patent.

21. I met the definition of a POSITA in 2011. 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 I am able to render opinions from the perspective of a POSITA based on my knowledge and experience.

IV. RELEVANT LEGAL STANDARDS

22. I am not an attorney. In preparing and expressing my opinions and considering the subject matter of the '138 patent, I am relying on certain basic legal principles that counsel have explained to me. These principles are discussed below.

23. I understand that prior art to the '138 patent includes patents and printed publications in the relevant art that predate the proper priority date of the alleged invention recited in the '138 patent.

24. 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.

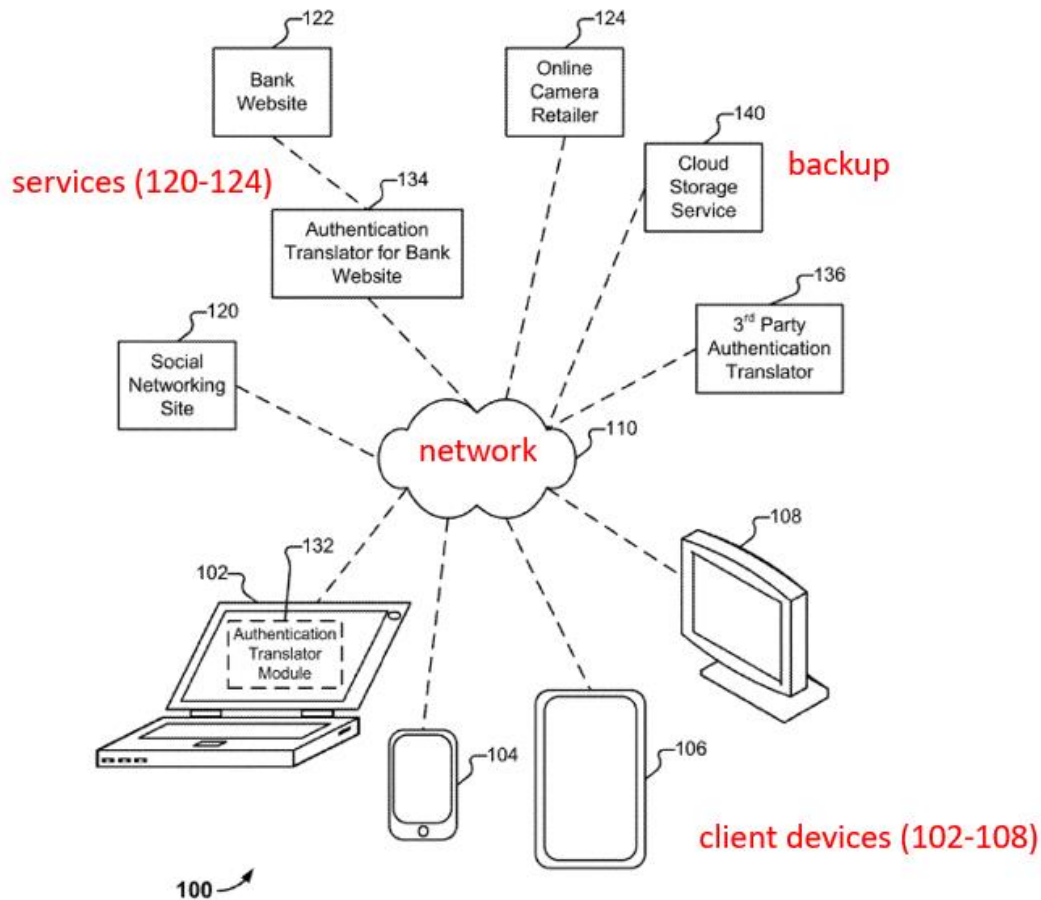
26. I further understand that certain factors may support or rebut the obviousness of a claim. I understand that such secondary considerations include, among other things, commercial success of the patented invention, skepticism of those having ordinary skill in the art at the time of invention, unexpected 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 '138 patent or any assignee of the '138 patent that any secondary considerations are relevant to the obviousness analysis of any Challenged Claim of the '138 patent.

V. OVERVIEW OF THE '138 PATENT

28. The '138 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 to a service such as a website. ('138 patent) APPL-1001, 2:40-61. FIG. 1 the '138 patent illustrates such an environment including client devices (102-108) connected to services (120-124).

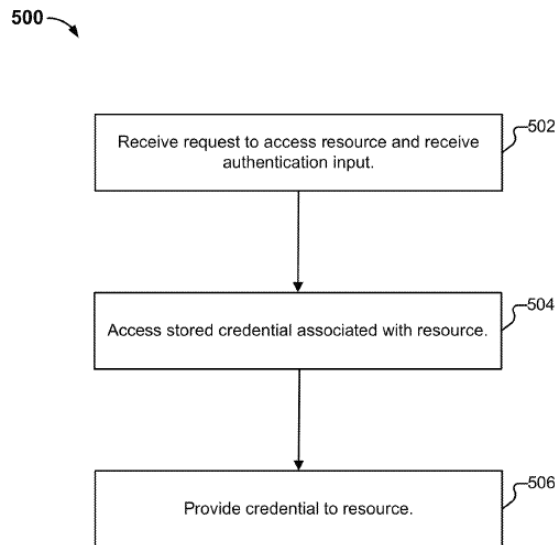


(’138 patent) APPL-1001, FIG. 1, annotated

29. The ’138 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. (’138 patent) APPL-1001, 1:37-46. The ’138 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.” ('138 patent) APPL-1001, 2:65-3:4.

30. FIG. 5 of the '138 patent illustrates a process for performing this authentication translation. ('138 patent) APPL-1001, 1:60-61.



('138 patent) APPL-1001, FIG. 5

31. The '138 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.” ('138 patent) APPL-1001, 6:33-42. 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. ('138 patent) APPL-1001, 6:50-56. If a match is found, a previously stored credential associated with the

resource is provided to the resource. ('138 patent) APPL-1001, 6:57-63.

32. I have reviewed the file history of the '138 patent, which I understand is attached as APPL-1002. The office first stated allowance of the subject matter of the '138 patent:

However, the references do not explicitly teach nor suggest in detail, ***facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and facilitate wiping of at least a portion of the at least one record*** in view of other limitations of the intervening claims.

APPL-1002, p. 182 (Office Action dated 11-2-2021 at pg. 4). After claims were indicated to be allowable, the applicant made revisions to the claims, which included replacing the “system” preamble of issued Claim 1 with “device” and removing a recitation of a “restricted interface” to read simply “interface” in each independent claim. APPL-1002, pp. 153-158, 170 (Interview Summary dated Nov 30, 2021, Response dated Sept 21, 2020).

33. However, the Examiner then provided another action rejecting the then pending claims as obvious over a combination of prior art; the Applicant responded with claim amendments as shown by representative prosecution claim 12 (which corresponds to issued claim 13):

12. (Currently amended) A method, comprising:

based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate, ~~using an interface~~, access of at least one record stored at least in part in a storage on the device, wherein the storage on the device is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device;

wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:

- a biometric template; and
- a credential comprising a cryptographic key;

in response to determining a match between a biometric input and the biometric template, retrieving, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, and wherein the biometric input is received subsequent to presenting of a prompt;

establishing a connection with the external resource;

facilitating a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and

facilitating, by the processor on the device, wiping of both the biometric template and the credential comprising the cryptographic key ~~at least a portion of the at least one record~~ stored at least in part in the storage on the device.

APPL-1002, p. 108. The Examiner again rejected the amended claims over a combination of art. APPL-1002, pp. 54-75 (Office Action dated May 13, 2022). And in response, the Applicant again amended its claims to include the recitation directed to “the prompt is visually presented:”

in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, [[and]] wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented:

APPL-1002, p. 41 (Response dated June 29, 2022). A notice of allowance issued with no additional reasons for allowance given. APPL-1002, pp. 8-15 (Notice of Allowance July 27, 2022).

34. However, prior to the '138 patent, it was well-known to a POSITA to perform all the elements of these claims including presenting prompts for biometric information visually. I discuss these elements in further detail below.

VI. TECHNOLOGY BACKGROUND

35. 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 '138 patent. The background below I discuss relevant technologies and techniques.

A. AUTHENTICATION

36. 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.

37. 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.

38. Well before the earliest 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.

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

B. CREDENTIALS AND CREDENTIAL MANAGEMENT

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

40. Long before the priority date of the '138 patent, authentication methods progressed from use of a simple password to provide additional security. Authentication systems, well before the priority date of the '138 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.

41. 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 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

42. 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.

43. A security architecture that commonly leveraged biometrics for authentication prior to the priority date of the '138 patent was “single sign-on” or

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>

SSO.³ In SSO, users initially login to a client device such as their computer through an authentication service relying upon password, hardware 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

44. 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

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

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

is) almost always stored in persistent storage (*e.g.*, on hard drives or in databases) in encrypted format—and thus protected from compromised systems.

C. CRYPTOGRAPHY

45. 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.

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

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

plaintext P from access by users who do not possess the decryption key Kd.

47. 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 HMACs in use at the time of patent included 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 priority date of the '138 patent.

D. CRYPTOGRAPHY IN WEB TRANSACTIONS

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

49. 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

encoded with either key, can be decoded using the other key.

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.

50. 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

51. 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.

52. By 2006, new computing systems with Trusted Platform Module (TPM) chips were being sold.⁶ A Trusted Platform Module (TPM) is a specialized microprocessor or hardware coprocessor that is designed to provide security-

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

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.

53. 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.

54. 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 priority date of the '138 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

55. It is my understanding that in order to properly evaluate the '138 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 the so-called *Phillips* standard, under which claim terms are given their ordinary

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>

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. “*processor*”

56. The ’138 patent states “[a]s used herein, the term ‘processor’ refers to one or more devices, circuits, and/or processing cores configured to process data, such as computer program instructions.” (’138 patent) APPL-1001, 2:21-23. A POSITA would understand that the plain and ordinary meaning of the term “processor” may include “one or more devices, circuits, and/or processing cores,” which includes a plurality of separate devices, circuits, and/or processing cores functioning together to provide to a processor.

B. “*restricted interface*” (*Claims 11, 23*)

57. A “*restricted interface*” is an interface that limits accessibility. In the ’138 patent specification, disclosure of such an interface is sparse. For an example device that “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),” the specification refers to access limitations in connection with an application

programming interface (API). ('138 patent) APPL-1001, 4:5-13 (“users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API”). At least in light of this, a POSITA would understand *restricted interface* to at least include an API that limits accessibility to secure storage, fingerprint sensor, or dedicated processor.

58. I have been told that the Patent Trial and Appeal Board (“Board”) has addressed this term, *restricted interface*, in other proceedings. In particular, I have been informed in a third-party IPR challenging US 10,824,696 (“the ’696 patent”), in which the Board found “[t]he specification of the ’696 describes only an ‘API’ (Application Programming Interface) as an example of a restricted interface between two processors.” IPR2022-00244, (Institution) Paper 17, 31 (PTAB 2002). I understand in IPR2022-00244, the Board referenced (in its description of the ’696 patent) the very same description noted above (from the ’138 patent). See IPR2022-00244, Paper 17, 8. In IPR2022-00244, the Board was ultimately persuaded a trusted platform module (TPM) architecture sufficiently disclosed the restricted interface recited in the ’696 patent. IPR2022-00244 Paper 17, 40 (relying on a TPM API stack depicted in Figure 7 of U.S. Pub. App. 2008/0059804 naming Shah). I agree that certainly interface(s) from the TPM architecture sufficiently disclose a *restricted interface*.

59. I understand that in parallel district court proceedings, Patent Owner

proposed (and the court issued a preliminary construction) the term *restricted interface* is to be understood in accord with plain and ordinary meaning. APPL-1026, 1. I demonstrate in the analysis that follows that the prior art renders obvious a *restricted interface* including an API that limits accessibility to secure storage, a fingerprint sensor, or a dedicated processor, an interface that limits accessibility, and a restricted interface under its plain and ordinary meaning. See *supra*, at VI.E (discussing trusted platform modules), (Challener) APPL-1007, 1:18-31.

60. Further, a POSITA would have understood a plain and ordinary meaning of the term *restricted interface* is an interface with limited accessibility. The interface may be physical or software. One example of such an interface that limits accessibility as is an API as the API defines the rules and protocols for communication between two applications (via the interface) and thus provides a restricted interface. TPM is a widely recognized security architecture that provides a *restricted interface(s)* as the architecture employs limited-accessibility, physical and software interfaces (APIs) to provide a restricted interface to security-related operations such as key and credential management, secure storage, encryption, decryption and digital signatures.

VIII. CLAIMS 1-3, 5, 7-8, 10-15, 17, 19, AND 22-25 ARE UNPATENTABLE

61. I have been asked to provide my opinion as to whether Claims 1-3, 5,

7-8, 10-15, 17, 19, and 22-25 of the '138 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 '138 patent.

62. 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 '138 patent.

63. 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	1-3, 7-8, 12-15, 19, and 24-25	§103(a) over Kesanupalli and Brown
#2	10, 22	§103(a) over Kesanupalli and Brown in further view of Cheng
#3	11, 23	§103(a) over Kesanupalli and Brown in further view of Challenger
#4	5, 17	§103(a) over Kesanupalli and Brown further in view of Headley

64. I understand from Counsel that the '138 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. As stated above, I have used the earliest possible priority date – Dec. 9, 2011 – for my analysis of this declaration. I understand from Counsel that each of Kesanupalli, Brown, Cheng and Challenger qualify as prior art with respect to this earliest possible priority date.

A. Ground 1: Claims 1-3, 7-8, 12-15, 19, and 24-25 are obvious under 35 U.S.C. § 103 over Kesanupalli and Brown.

1. Summary of Kesanupalli

65. 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).

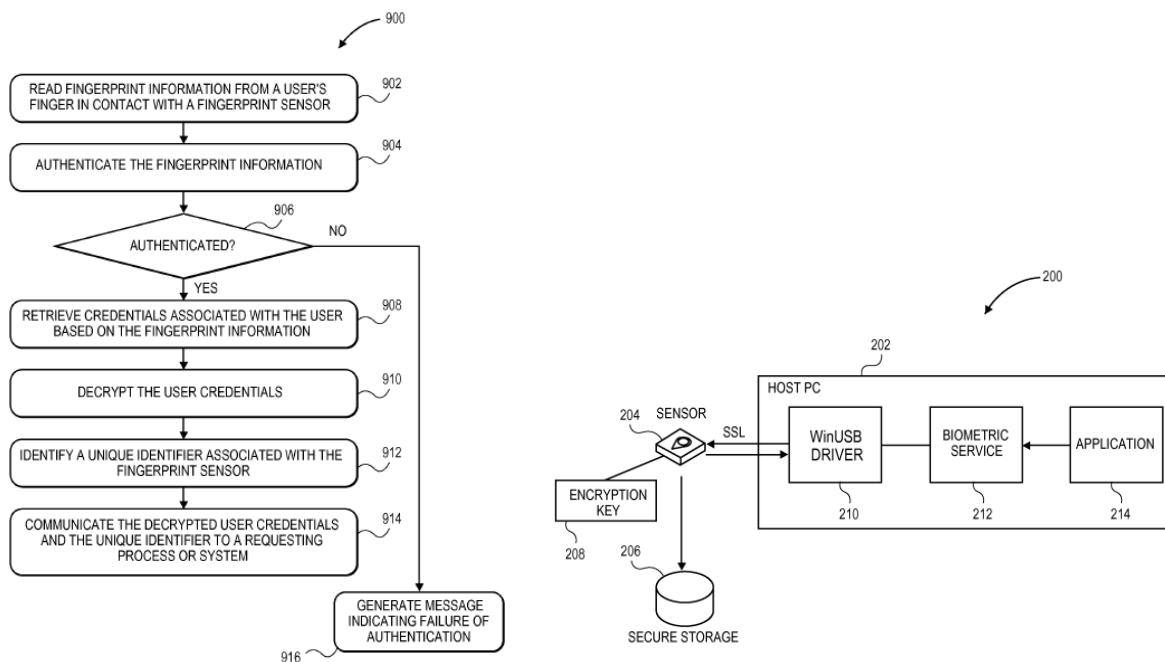
66. Kesanupalli is directed to a secure authentication system that uses biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” (Kesanupalli) APPL-1006, 1: 59-62. For example, based on a match between a fingerprint template 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, 3:14-4:11. Credentials are discussed above

at Section VI.B.

67. 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, 8:29-53.

68. 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,” such as a “cryptographic key.” (Kesanupalli) APPL-1006, 3:62-4:1, 3:41-44, FIG. 12.

69. 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.



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

70. 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.

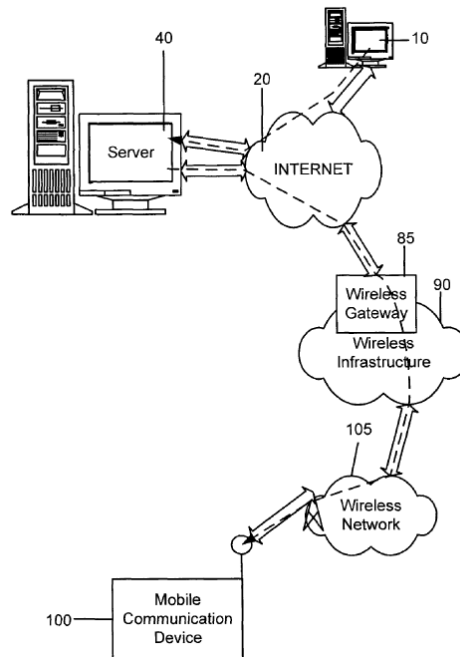
(Kesanupalli) APPL-1006, FIG. 2, 5:9-58, 6:11-31.

2. Summary of Brown

71. U.S. Patent No. 9,652,629 to Brown *et al.* (“Brown”) issued on continuation of an application that was itself a continuation of an application filed on January 18, 2008 and is entitled “Selectively Wiping a Remote Device.” (Brown) APPL-1009, (63), (54).

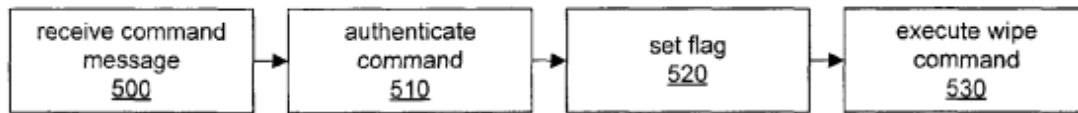
72. Brown “relates generally to the field of computer and network security, and more particularly, to wiping data stored on a remote device such as a mobile communication device.” (Brown) APPL-1009, 1:15-18.

73. FIG. 1 of Brown “shows a first communication device, here a client personal computer 10, a network, herein the Internet 20 ... and a second communication device, here a client mobile communication device 100.” (Brown) APPL-1009, 4:60-64. The client devices may be personal computers, mobile devices, mobile communication devices, communication devices, computing devices, or data storage devices” such as “laptop and notebook computers, PDAs, smartphones, and the like.” (Brown) APPL-1009, 4:54-65.



(Brown) APPL-1009, FIG. 1

74. Brown recognizes the client devices include “data of a sensitive or critical nature” that is desired to be protected from “unauthorized or malicious users” in cases when the client’s device is “compromised, decommissioned, or redeployed.” (Brown) APPL-1009, 1:15-2:17. Brown provides for protecting the data in such instances by wiping the data from the client device such that it is deleted from the device and cannot be retrieved. Brown illustrates in its FIG. 6 “a flowchart depicting a sequence of steps in the execution of the wipe command on the client device 10, 100” where the command may be invoked by at the device, such as by failing a predetermined policy (*e.g.*, incorrectly entering an authentication credential at the device a given number of times) and/or may be invoked by a remote server. See (Brown) APPL-1009, 11:65-13:14.



(Brown) APPL-1009, FIG. 6

3. Reasons to Combine Kesanupalli and Brown

75. A POSITA would have been motivated to apply Brown’s teachings of selectively wiping sensitive data from storage of a device such as the storage used in Kesanupalli to store biometric information associated with a user and credentials for user authentication to resources such as websites. Kesanupalli’s stored biometric information and credentials are sensitive data and applying Brown’s selectively wiping teachings would produce the obvious, beneficial, and predictable results of reducing the risk of unauthorized or malicious user access to that sensitive data on a lost or stolen device. I discuss this below including that wiping data is deleting data, which is advantageous to protect the data from unauthorized use if the user’s client device is no longer under the user’s control.

76. **First**, Kesanupalli, Brown and the ’138 patent are analogous art and are all in the same field of endeavor—information security, and more particularly, security arrangements for protecting computers or other electronic devices, components thereof, programs or data against unauthorized activity. *See, e.g.*, (Kesanupalli) APPL-1006, 2:30-38 (“[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”); (Brown) APPL-1009, 1:10-19 (“[D]isclosure relates generally to the field of computer and network security [including] [d]ata stored in the memory of a communication and/or computing device, such as a mobile communication device, personal digital assistant (PDA), smartphone, laptop computer, and the like, [that] may include data of a sensitive or critical nature that is accessible only by authorized users.”); (’138 patent) APPL-1001, 1:37 (“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).

77. Moreover, I note from the front page of Kesanupalli, Brown and the ’138 patent, 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 which I am informed is: security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. See (’138 patent) APPL-1001,

(51), (52); (Kesanupalli) APPL-1006, (51) (58); (Brown) APPL-1009, (51), (52).

78. Both Kesanupalli and the '138 patent are directed to biometric authentication including the secure storage of the personal data that is required to perform this authentication, and associated user credentials. *See, e.g.*, (Kesanupalli) APPL-1006, FIG. 9, '138 patent, FIG. 5. Brown similarly is directed to systems for securing client devices that include “data of a sensitive or critical nature” such as data files personal to the user including “authentication processes” (Brown) APPL-1009, 1:15-2:8. Moreover, Brown discusses implementing its disclosure in systems in the context of providing authentication services such as password management. *See* (Brown) APPL-1009 at 6:4-31.

79. Second, a POSITA would have been motivated to employ Brown’s wiping technique in connection with Kesanupalli’s secure user authentication methods because Kesanupalli’s stored biometric information and credentials are sensitive data. A POSITA would have understood the stored biometric information and credentials would be at risk if Kesanupalli’s device were lost or stolen. Such a problem would have also been reasonably pertinent to the inventor of the challenged patent. *See* ('138 patent) APPL-1001, 8:30-35 (noting that “criminals with physical component access to lost devices [could] gain access” to sensitive information). Brown teaches that, though data stored on a device “may be protected by requiring the user to enter a valid password in order to access

applications or data on the device, or by encrypting data stored on the device such that access to the data requires decryption by a valid decryption key, there are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or ‘wipe’ data.” (Brown) APPL-1009, 2:6-13. Thus, not only were Kesanupalli, Brown and the ’138 patent in the same field of endeavor, but Brown would have been reasonably pertinent to a problem faced by the inventor of the ’138 patent and pertinent to known risks of theft and loss that a POSITA would have been motivated to address in the Kesanupalli-Brown combination.

80. In particular, a POSITA would readily recognize a personal electronic device can be compromised such as when a component is lost, damaged, or otherwise require replacement. *See* (Kesanupalli) APPL-1006, 10:13-18; (Brown) APPL-1009, 2:11-15 (“[T]here are instances when the device may be compromised, decommissioned, or redeployed, making it desirable to delete or ‘wipe’ data, including applications, on the communication device so that it cannot be accessed by unauthorized or malicious users.”) The need to protect data, such as completely limiting access to the data, when the device is compromised is evident. Moreover, a POSITA would have recognized a desire in the market of

electronic devices to be capable of being wiped long before the '138 patent.⁹

Brown recognizes that while data may be protected by authentication procedures and encryption, additional protection may be desired. *See* (Brown) APPL-1009, 1:28-35, 1:66-2:9. It is a standard practice to provide multiple layers of protection for a user's data. Brown's system and method for wiping data at a communication device (including according to a predefined rule) would be a readily recognized advantage to the client devices of Kesanupalli – that of protecting data on the client device from unauthorized use by wiping it from the device. Simply put, if the data is wiped or deleted from a device to which a user no longer has control, the data is unavailable for malicious or unauthorized users who may gain control of the physical device. This is particularly the case when the data is personal in nature, such as the records of Kesanupalli.

81. Finally, a POSITA would have had reasonable expectations of success in adding a wipe feature such as taught by Brown in a biometric authentication system such as taught by Kesanupalli, as Brown is similarly directed

⁹ *See* (Cheng) APPL-1008, [0006] (“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...”)

to improving security of personal information. Adding a wipe 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 wiping technique of Brown is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices.

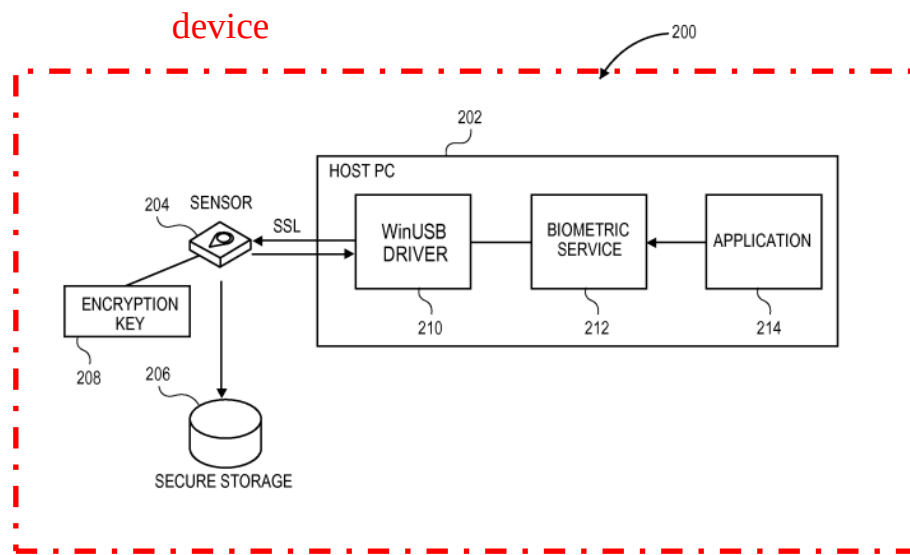
82. In particular, Brown discloses a processor facilitates its wiping techniques. See APPL-1009, 4:9-50 (“a mobile client device for selectively securing data from unauthorized access of the client device...the device comprising a processor...the processor may be configured to secure the data by deleting the data corresponding to each of the plurality of data types thus determined in the memory...”), 9:12-38, 21:1-48; FIG. 2, 7:47-55. The processor of Kesanupalli is operable to receive instructions to execute the wiping functions performed by Brown's processor. And implementing a wiping technique is a predictable task easily accomplished by Kesanupalli's processor, which is readily capable of, for example, overwriting data as discussed in Brown.

4. Claim 1

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

83. Kesanupalli discloses *a device* according to Claim 1 relative to this limitation and limitations that follow.

84. Kesanupalli describes relative to its FIG. 2 a device “capable of performing biometric user enrollment and authentication.” (Kesanupalli) APPL-1006, 2:1-2.



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

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 communicate user credentials to web servers. (Kesanupalli) APPL-1006, Abstract, 2:54-3:3, 4:3-11, 4:36-50, 6:11-49.

85. In the claim, *device* is recited as a generalized collection of components, as in “[a] *device, comprising: a processor on the device ...; a storage on the device ...; and a memory coupled to the processor ... (see also, infra [1.1],*

[1.2], [1.9]), while at the same time, the '138 patent specification lexicographically defines the term “processor” in a generic manner as “one or more devices, circuits, and/or processor cores configured to process data, such as computer instructions.” ('138 Patent) APPL-1001, 2:21-23.

86. A POSITA would appreciate that Kesanupalli's embodiment illustrated in FIG. 2—and likewise embodiments described relative to FIGs. 1 and 6—constitute such a device, generically defined. Nonetheless, to the extent that Patent Owner imparts 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.”)

87. Thus, Kesanupalli discloses *a device*, as claimed.

b) [1.1] *a processor on the device*;

88. Kesanupalli discloses *a processor on the device*.

89. As explained in [1.0] and in Section VII.A, the '138 patent specification lexicographically defines the term “processor” in a generic manner as “one or more devices, circuits, and/or processor cores configured to process data, such as computer instructions,” see ('138 Patent) APPL-1001, 2:21-23, while at the same time establishing that the recited processor is on the *device*, which comprises such a *processor*, *storage* and *memory* (see also, *infra* [1.1], [1.2], [1.9]).

Accordingly, a POSITA would understand the recited *processor* to encompass circuits, processor cores and indeed devices that process data such as computer instructions within the construct of the larger device in (or on) which they reside.

90. Similarly, a POSITA would understand Kesanupalli to include such a *processor* on the device that includes sensor 204 and PC 202. Kesanupalli describes what a POSITA would readily recognize, its functions of authentication translation and communication with external resources are performed by a such *processor*, broadly defined:

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.

91. As illustrated in the citation above, Kesanupalli suggests both specialized and generalized processor circuitry may be used to effectuate its authentication translation methods and devices. In particular, it would be recognized that Kesanupalli is implemented using specialized processing circuitry executing the authentication functions, such as performed by the sensor 204, and general processing circuitry executing the functions of communicating with an external resource (HOST PC 202). 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. 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 a *processor on the device* as according to the '138 patent, a processor can include more than one circuit, device or core as discussed above. See ('138 patent) APPL-1001, 2:21-23.

92. To the extent that the Patent Owner argues that the processing circuitry must be implemented as single processor, such as a single chip or single module, a POSITA would also recognize such implementations to be obvious in view of Kesanupalli's disclosure of the functions to be executed. For example, one form of *processor on a device* suitable and readily configurable to provide processing circuitry for executing the functions of both the sensor 204 and the PC 202 is system on a chip (SoC). In an SoC implementation, a processor core or cores providing processing integrated circuitry for executing the functions of the PC 202 together with specialized circuitry, programmed devices or even additional processor cores to execute other specialized functions such as that of sensor 204 and its secure storage 206. SoCs were in use well before the effective filing date of

the '138 patent.¹⁰

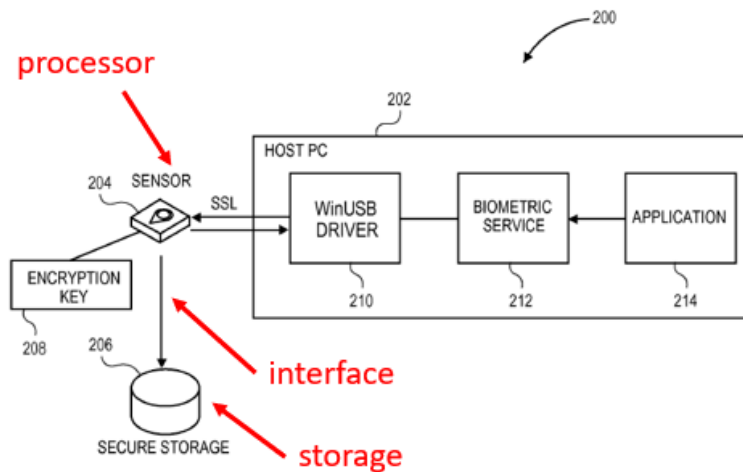
93. Thus, Kesanupalli discloses *a processor on the device*.

c) [1.2] *a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device,*

94. Kesanupalli discloses *a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device*.

95. Kesanupalli illustrates a secure storage 206, which provides a *storage on the device*. See (Kesanupalli) APPL-1006, 2:48-50, 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.”), 6:45-47.

¹⁰ See, e.g., APPL-1018, <https://www.eetimes.com/introduction-to-programmable-systems-on-a-chip/>



APPL-1006, FIG. 2, annotated

96. As illustrated in FIG. 2 above, secure storage 206 is accessible by the processor circuitry executing the functions of sensor 204 as shown by the vertical arrow extending from the sensor 204 to the storage 206. This is confirmed by Kesanupalli's disclosure, which I discuss in detail below (e.g., limitations [1.3] and [1.7] respectively) where the processor accesses the storage 206, in order for the sensor 204 to perform authentication, which includes matching a biometric input with a biometric template in the storage 206, and thus requires accessing the storage for the biometric template; and also in order to release user credentials located in the storage 206 upon a successful match. See, e.g., FIG. 9 which illustrates at block 904 and 908 the access of the storage by the processor (sensor 204).

97. FIG. 2 illustrates the processor accesses the storage 206 via *an interface that facilitates communication* between the secure storage 206 and the process – and in particular the processor circuitry of sensor 204 as annotated above.

98. As discussed in limitation [1.1], POSITA would understand Kesanupalli provides a processor on the device that executes its functions including of sensor 204, and as such it is the *processor* that accesses the memory 206. In particular, a POSITA would understand that Kesanupalli’s description of the “sensor 204” accessing the secure storage 206 means it is the processor circuitry of the sensor 204 that accesses the storage 206; this is the known function of a processor as explained by Kesanupalli: “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.

99. Each time the processor accesses the secure storage 206 it does so via the *interface*, as access to the storage 206 is the only disclosed connection to the storage 206 (*see* highlight in FIG. 2 above). 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. The processor (and in particular the processor circuitry executing the functionality of sensor 204) accesses the storage 206 in order to perform the function of determining a match between a biometric template stored in secure storage 206 and a user’s biometric input to the sensor 204. (Kesanupalli) APPL-1006, 6:42-46. In order for the processor to determine a match with a stored template, the processor accesses the secure storage 206 to access the template and does so by communication via the *interface* highlighted above. The processor (and in particular the processor circuitry executing the functionality of sensor 204) also accesses the storage 206 to retrieve user credentials to release the credentials upon a successful match. On a match, the user credentials are communicated between

the storage 206 to the processor such that they can be sent to a requesting service.

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. The user credentials are communicated between the storage 206 on the device and the processor (in particular, the processor circuitry executing the functionality of sensor 204) as the user credentials are provided to an external resource. *See also*, (Kesanupalli) APPL-1006, FIG. 2, 3:52-4:12, 5:17-32, 8:40-53, 9:4-9, 9:17-24, FIG. 12. Thus, the interface between the processor circuitry executing the functionality of sensor 204 and the secure storage 206 is an interface that facilitates communication between the storage on the device and the processor on the device.

100. Thus, Kesanupalli discloses this element.

d) [1.3] *wherein the processor on the device is configured to: based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;*

101. Kesanupalli discloses *the processor on the device is configured to: based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device.*

102. As described above with reference to element [1.1] and in view of the '138 patent specification's use of the term *processor* in a generic manner as "one or more devices, circuits and/or processor cores configured to process data,

such as computer instructions,” a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute the *processor on the device*. Kesanupalli and, in combination, Brown disclose the functionality, *i.e.*, the processing, that the *processor on the device* is configured to perform and that functionality is described with reference elements [1.3] - [1.8].

103. As discussed below, the elements of claim 1 were known in the art as illustrated in Kesanupalli (see Section VIII.A.1) and Brown (see Section VIII.A.2). Further I note the features of claim 1 provide for performing functions that were well known fundamentals of the relevant technology as discussed in VI.A-E.

104. Turning first to element [1.3], Kesanupalli describes an enrollment in an external resource such as a website in which *at least one record is stored in at least part in the storage on the device*. As discussed below, the *record* includes user’s credential (*e.g.*, cryptographic key) and biometric template, which are bound and stored in the secure storage 206:

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, 3:15-51. Kesanupalli in FIG. 7 walks through this enrollment process. APPL-1006, 8:29-53 (including block 710 where “the procedure binds the user credentials with the fingerprint template[], then stores the user credentials and the fingerprint template [] in a secure storage.”) *See also*, (Kesanupalli) APPL-1006, FIG. 2, 4:36-5:43, 3:65-4:1, 5:35-43, FIG. 12, 8:6-22. FIG. 11 of Kesanupalli also illustrates dataflow in an enrollment process. Kesanupalli describes that this record is associated with a particular external resource (*e.g.*, website):

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, 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...”). Kesanupalli’s biometric template and user credential constitute a *record* as they are bound and stored in the secure storage 206 as I discuss below.

105. 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 is 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

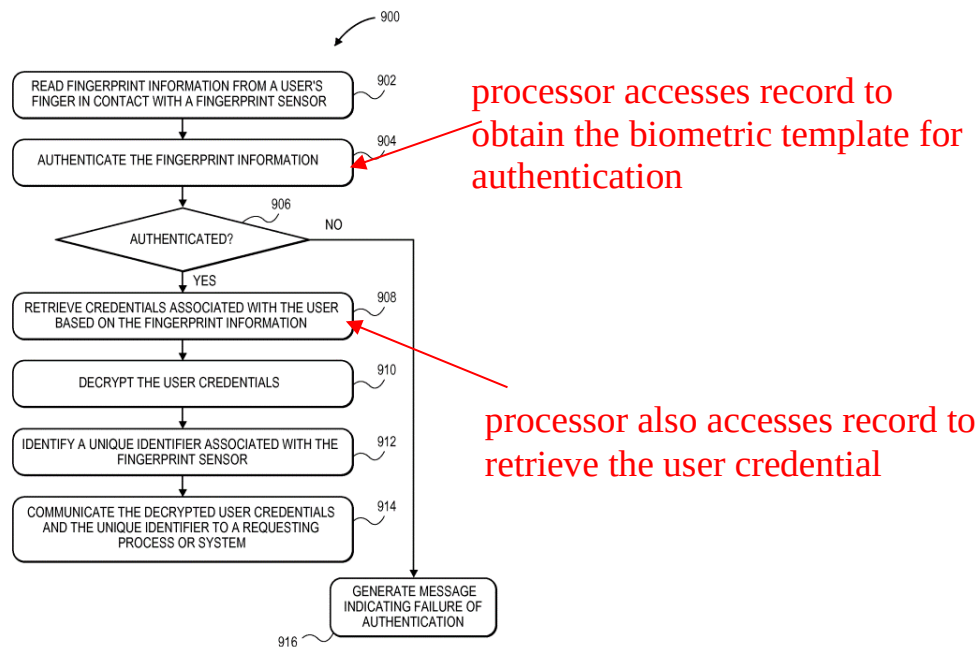
file in storage, or a row of a table in a database. This grouping allows for the representation of in a structured and organized manner and simplifies the program code and prevents bugs. A POSITA would understand Kesanupalli's biometric template and user credential to be associated data that is stored and referenced together (in the secure storage), and thus would be represented as a record.¹¹

106. After enrollment including the creation and storage of the record, subsequent visits by the user to the external resource initiate an authentication translation procedure. APPL-1006, 5:9-14 (“After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits cause...the Web site [to] prompt[s] the user to perform user authentication.”) This authentication process is *based at least in part on a request from a user to access an external resource* (i.e., the visit to the website with which the user has previously enrolled) and includes the processor *accessing* the record in storage to perform the authentication. The processor accesses the record in storage in order to obtain the biometric template for matching with the user's input in the authentication process. *See also*, APPL-1006, FIGS. 8, 9, 3:51-4:1, 8:54-9:24, FIGS. 8, 9, 12. FIG. 9 is illustrative of the procedure for authenticating a user after she has enrolled in a website.

¹¹ *See, e.g.*, APPL-1019, entry “data 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.

**APPL-1006, FIG. 9, annotated**

107. In particular with respect to the device of FIG. 2 in the authentication process, the *processor* (sensor 204) *facilitates access* to the storage 206 using its *interface* to the storage 206 to obtain the biometric template of the record of the storage 206 such that the processor can determine matching of biometric input to said template, and again facilitates access to the storage 206 to access the user credential of the record to release the credential to the external resource using the application 214 of the PC 202 on a successful match. (Kesanupalli) APPL-1006, FIG. 2, 3:44-51, 6:42-49, FIG. 12. Simply put, the authentication and subsequent release of credentials is performed based on the user's visit and request to gain access to an external service with which she has enrolled. See (Kesanupalli), APPL-1006, FIG. 12 "User."

108. The processor, and in particular the circuitry executing the functions of sensor 204, facilitates the access of the biometric template of the record *using the interface* between the processor circuitry executing the functions of sensor 204 and the secure storage 206 where the template is stored. (Kesanupalli) APPL-1006, FIG. 2, 3:44-51, 6:45-49. If authenticated, the processor circuitry executing the functions of sensor 204 retrieves the user credentials associated with the requested external resource from the record and communicates the user credentials to the PC 202, and application 212 of PC 202 communicates the credentials “to the Web site to complete the user authentication process.” (Kesanupalli) APPL-1006, 5:22-24. *See also*, FIG. 12. The processor circuitry executing the functions of sensor 204 facilitates the access of the user credentials of the record *using the interface* between the processor circuitry executing the functions of sensor 204 and the secure storage 206 where the credentials are stored. (Kesanupalli) APPL-1006, FIG. 2, 3:44-51, 6:45-49. Thus, the processor executing the functions of sensor 204 *accesses* the biometric template of the record for performing this comparison; and also *accesses* the user credentials of the record stored to release the user credentials upon determining a match in biometrics. *See* (Kesanupalli) APPL-1006, 3:52-4:12, 5:17-32, 8:40-53, 9:4-9, 9:17-24, FIG. 12.

109. Processor circuitry executing the functions of PC 202 receives the user’s request from the external resource and receives the user’s the credentials

from the sensor 204 and communicates them to the external resource in response to said user's request. The processor executing the functions of PC 202 facilitates access of the record in secure storage 206 using an interface between the PC 202 and the sensor 204 as it receives communication from the processor executing the functions of sensor 204 via this interface. (Kesanupalli) APPL-1006, FIG. 2, 6:39-42 ("The biometric sensor 204 creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique.")

110. Thus, Kesanupalli discloses this element.

e) [1.4] ***wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key;***

111. Kesanupalli discloses *the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key.*

112. As discussed above in [1.3], Kesanupalli's processor (including devices/circuits/processing cores executing functions of sensor 204) is configured to access of the *at least one record is associated at least with the external resource (e.g., website).* Also as discussed in [1.3], *the at least one record comprises: a biometric template; and a credential comprising a cryptographic key.*

Kesanupalli's biometric template and user credential constitute a *record* as they are bound and stored in the secure storage 206, i.e., stored together in a data structure,

see above. The user credential and the bound template is a *record associated at least with the external resource* as it is a token specific to the particular external resource such as a website. (Kesanupalli) APPL-1006, 5:33-43 (“different user credentials are associated with each Web site with which the user enrolls”).

113. In particular, Kesanupalli describes in its enrollment “a user swipes their finger across the fingerprint sensor several times to create a fingerprint template.... After creating a fingerprint template, the user (or a web server or other system) provides user credentials, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein bind the user's fingerprint template with the user credentials. The fingerprint template and user credentials are then stored in a secure storage device.” (Kesanupalli) APPL-1006, 3:32-51. The fingerprint template is one type of “biometric template” suggested by Kesanupalli. (Kesanupalli) APPL-1006, 3:15-18 (“a user enrolls...by binding their user credentials with the user’s biometric template (a ‘fingerprint template’ in specific implementations.”)

114. Kesanupalli’s user credential and bound biometric template is a *record associated at least with the external resource* as it is a token specific to the particular external resource such as a website. APPL-1006, 5:33-43 (“different user credentials are associated with each Web site with which the user enrolls”). Kesanupalli also describes one type of user credential is a *cryptographic key* as the

user credentials may be a “password, cryptographic key, random seed, and the like.” APPL-1006, 3:32-51, *see also*, 3:65-4:1, 5:35-43, FIG. 12, 8:6-22.

115. Thus, Kesanupalli discloses this element.

f) [1.5A] *in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature,*

116. Kesanupalli discloses *in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature.*

117. As described above with reference to element [1.1], a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform and that functionality is now described relative to the limitations of element [1.5A].

118. First, Kesanupalli describes receiving a *biometric input*. In one example, Kesanupalli describes the sensor (sensor 204) receives a biometric input of a fingerprint from a “fingerprint sensor.” (Kesanupalli) APPL-1006, 6:31-36.

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).”).

119. Kesanupalli authentication process describes *in response to determining a match between a biometric input and the biometric template, retriev[ing], from the at least one record, the credential*. Continuing with the discussion of FIG. 9, Kesanupalli describes:

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) ...

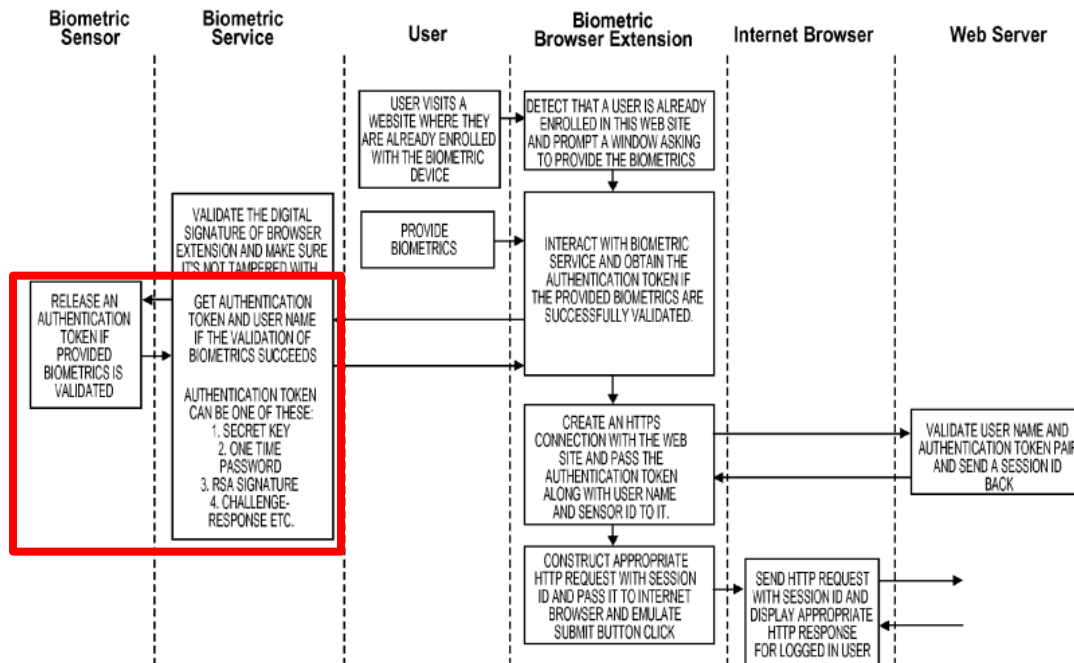
(Kesanupalli) APPL-1006, 9:14-20. Authenticating, or validating, a biometric input such as a fingerprint is matching the fingerprint to the stored biometric template.

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, 3:52-4:12 (including “3:52-56 (“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,” 5:17-32, 8:40-9:25, FIGS. 8, 9. FIG. 12 of Kesanupalli is illustrative of actions for

identifying and authentication of a user, which includes the actions performed by a “user,” actions performed by the components of the user’s device—sensor (e.g., by sensor 204 shown at left) and applications of the PC (e.g., PC 202 providing biometric service, browser extension, browser applications)—and the external resource’s web server. (Kesanupalli) APPL-1006 2:22-24, 9:52-57.



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

120. Kesanupalli describes the *processor on the device* performs the steps above of retrieving the credential as the sensor 204 is accessing the storage 206, performing the matching of the input and template and if a match is found releasing the credential for transfer to a requesting processor system by the application of PC 202. See APPL-1006, 6:11-25, 6:31-49, 9:10-24. The processor

executing the functions of PC 202 retrieves the credential from the sensor 204 and communicates the user credential to the external resource. See (Kesanupalli) APPL-1006, 3:52-4:12, 5:17-32, 8:40-53, 9:4-9, 9:17-24, FIG. 12.

121. To the extent the Patent Owner argues that the processor is also to perform the determining a match between a biometric input and the biometric template, the processor circuitry of sensor 204 performs the matching. (Kesanupalli) APPL-1006, 6:31-49.

122. Kesanupalli also describes *biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, or a feature usable for a retina scan:*

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.

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, 6:31-36.

123. Thus, Kesanupalli discloses this element.

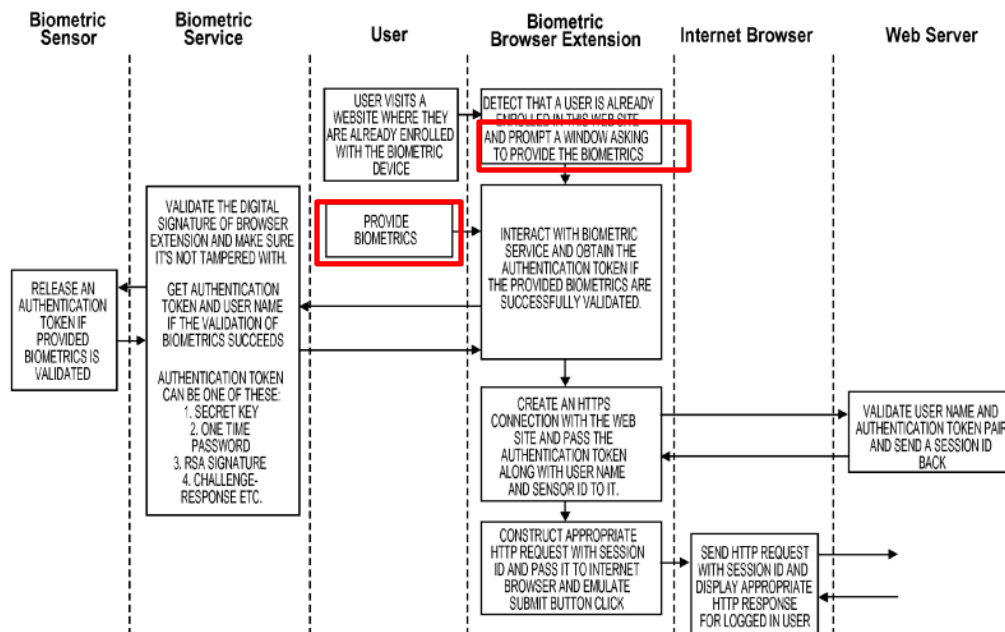
g) [1.5B] *wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;*

124. Kesanupalli discloses *the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented.*

125. First, Kesanupalli discloses *the biometric input is received subsequent to presenting of a prompt:*

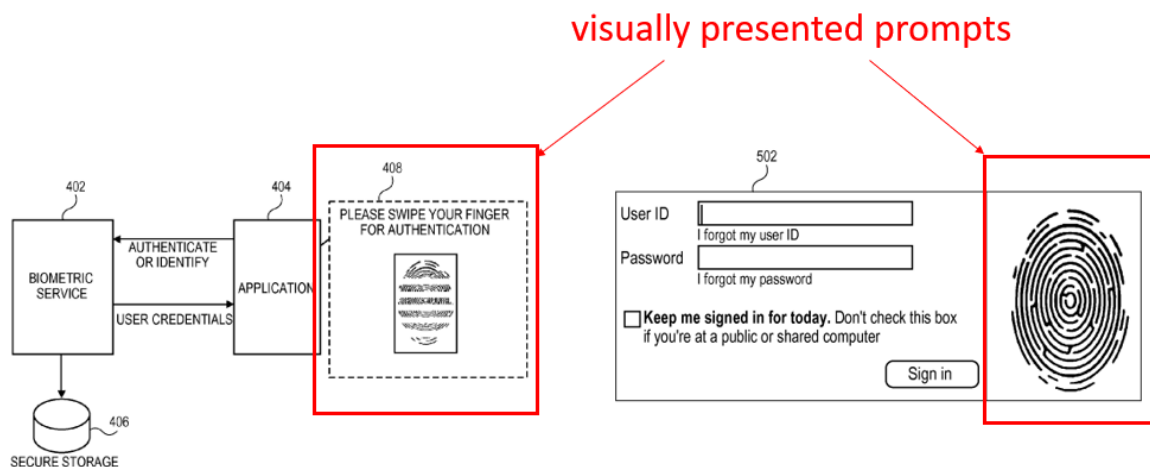
After a user has enrolled with a particular Web site that supports biometric authentication, subsequent visits to the same Web site cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication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

(Kesanupalli) APPL-1006, 5:9-14.



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

126. Kesanupalli also describes that this prompt can be *visually presented* as illustrated in FIGS. 4 and 5 and the accompanying descriptions.



(Kesanupalli) APPL-1006, FIGS. 4 and 5, annotated

See (Kesanupalli) APPL-1006, 7:1-16 discussing FIG. 4 including “Application

404 initiates the user authentication process by displaying a request 408 for the user to provide their fingerprint (in the case of a fingerprint sensor).”; 7:17-24 discussing FIG. 5 including “example user login interface 502 displayed during the user authentication process. The example of FIG. 5 requests a user ID and a password, then asks the user to provide biometric information...” A user interface that is “displayed” and in particular, a request for the user to provide their input that is “displayed” is *visually prompted*.

127. Thus, Kesanupalli discloses this element.

h) [1.6] *establish a connection with the external resource;*

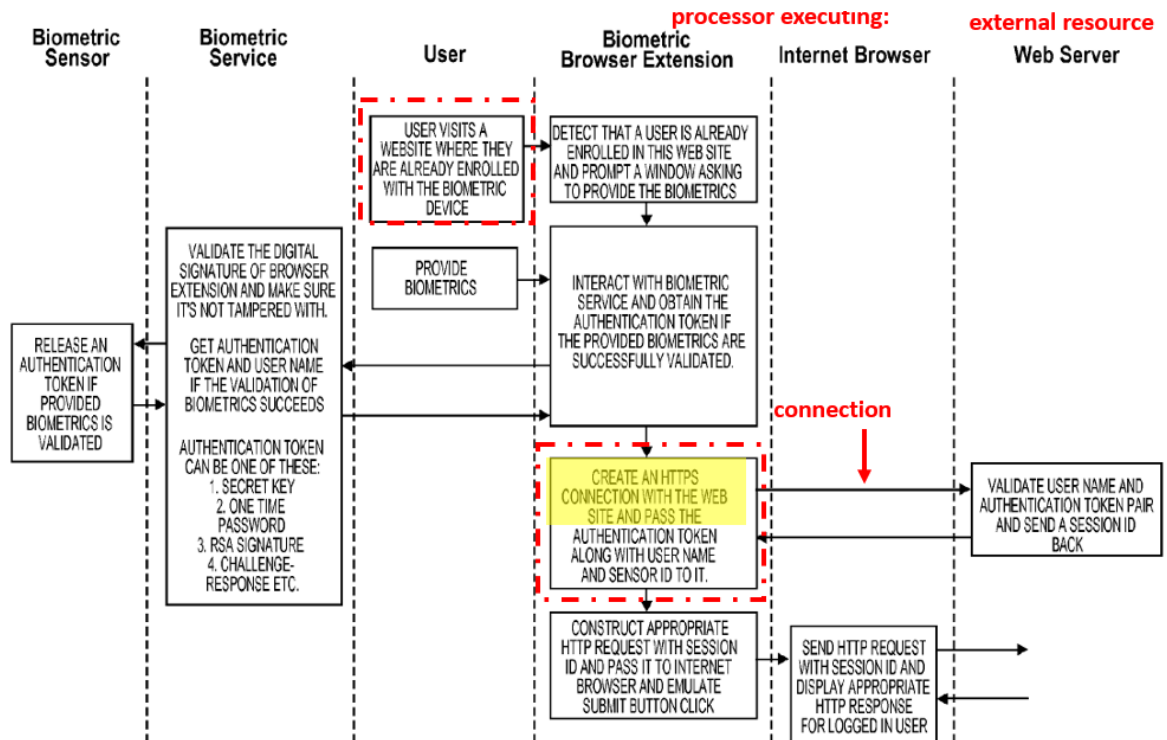
128. Kesanupalli discloses *establish[ing] a connection with the external resource*.

129. As described above with reference to element [1.1], a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform and that functionality is now described relative to the limitations of element [1.6].

130. In Kesanupalli, the processor on the device, in particular, the processor circuitry executing the functions of the PC 202, establishes a connection with the external resource (website).

As used herein, a “web application”, a “web-based application”, and a “web-enabled application” refers to a software application or software routine that is capable of communicating with one or more web servers or similar devices via the Internet or other data communication network. Additionally, a “plug-in” or a “browser plug-in” refers to an application or extension that provides a variety of different features and functions. Particular examples of “plug-ins” and “browser plug-ins” discussed herein provide features and functions related to user authentication while, for example, accessing web sites, making secure transactions, and the like.

(Kesanupalli) APPL-1006, 2:54-3:3. *See also*, (Kesanupalli) APPL-1006, 4:36-5:43, 6:11-50, 7:25-32, 7:67-8:4, 9:58 – 10:1. With respect to the device of FIG. 2, based on the user’s request to access the website, application 214, which is executing on a processor circuitry of the PC 202 communicates, via the Internet, with a webserver of the website. (Kesanupalli) APPL-1006, 6:11-31, FIG. 9, block 914. FIG. 12 is illustrative of the actions and functions:



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

Kesanupalli describes the connection between the PC and the webserver as a “secure communication link,” which is a *connection*. (Kesanupalli) APPL-1006, 7:54-8:5, 12:62-67.

131. Both Kesanupalli and the ’138 patent describe their communication of credentials to website in terms of SSL (now TLS) or HTTPS protocols.

- (’138 patent) APPL-1001, 5:18-25 (“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 '138 patent describe communication of a decrypted credential to the website via a *connection establish[ed]* in like manners.

132. Thus, Kesanupalli discloses this element.

i) [1.7] ***facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and***

133. Kesanupalli discloses *facilitat[ing] a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output.*

134. As described above with reference to element [1.1], a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores

that constitute the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing that the *processor* is configured to perform and that functionality is now described relative to the limitations of element [1.7].

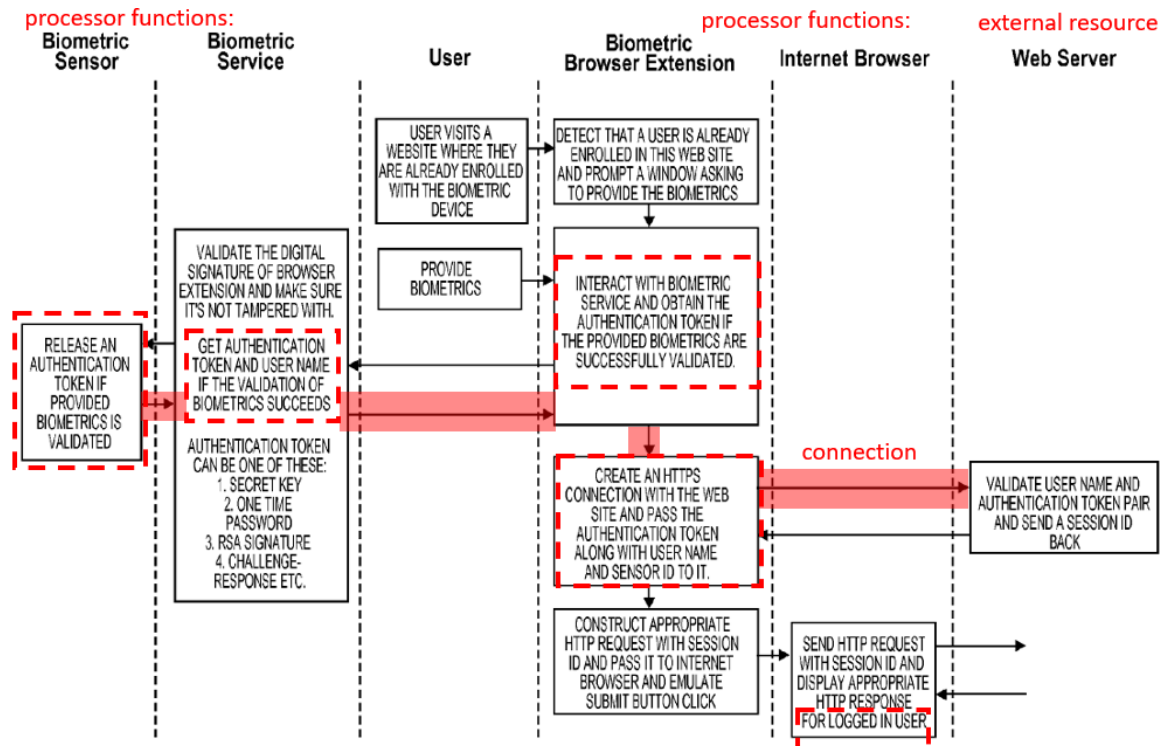
135. In Kesanupalli's device, the processor *facilitates a login of the user to the external resource* (e.g., website) *at least in part by transmitting, via the established connection* (e.g., connection between PC 202 (application 214) with the web server), *output* (e.g., the user credential) *based at least in part on the credential retrieved from the at least one record*. First, Kesanupalli describes its processor performs *transmitting output* (the user credential itself) 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*, (Kesanupalli) 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 212 of PC 202 for communication to the external resource. (Kesanupalli) APPL-1006, 6:11-49.

FIG. 12 annotated below illustrates transmitting user credentials to an external resource.



APPL-1006, FIG. 12, annotated

Kesanupalli's transmitting the decrypted user credential is *transmitting ... output based at least in part on the at least one the password or the cryptographic key as*

it is output consisting of the (decrypted) user credential (cryptographic key).¹²

136. As discussed in element [1.6], a connection is established between the device (in particular the processor executing the functions of PC 202) and the external resource. The application 212 of the PC 202 communicates the decrypted credential to the website via this *established connection*. See (Kesanupalli) APPL-1006, FIG. 2, 3:52-65, 4:3-5, 4:51-63, 5:59-6:49, 8:6-18.

137. The output of the user credential to the external resource *facilitates a login of the user to the external resource* because based at least in part on the output of the user credential, the user is *logged in* to the external resource. A POSITA would understand when Kesanupalli communicates the credentials “to the Web site to complete the user authentication process,” the user is logged in. See (Kesanupalli) APPL-1006, 5:22-24. See also, (Kesanupalli) APPL-1006, FIG. 12 (“logged in user”). This is the point of Kesanupalli’s authentication procedures and transmittal of the credential to the website, to provide the user access to the resource (e.g., to provide for a log in).

138. Thus, Kesanupalli discloses this element.

¹² In a joint claim construction statement, the parties agreed the construction of this clause is plain and ordinary meaning including “that ‘the output does not need to include the credential’.” APPL-1026, 3.

j) [1.8] *facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and*

139. Kesanupalli in combination with the teachings of Brown discloses *facilitat[ing] wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device.*

140. As described above with reference to element [1.1], a POSITA would understand Kesanupalli to describe the devices, circuits and/or processing cores that constitute the *processor on the device*. Kesanupalli also discloses and renders obvious the functionality, *i.e.*, the processing, that the *processor* is configured to perform and that functionality is now described relative to the limitations of element [1.8].

141. As discussed above, Kesanupalli discloses storing at least one record in the storage on the device, and that this record includes the biometric template bound with the user credential (*e.g.*, cryptographic key).

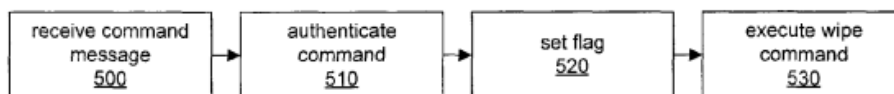
142. As discussed above, Kesanupalli discloses storing at least one record, the biometric template bound with the user credential (*e.g.*, cryptographic key), in the storage on the device. It would have been obvious for the processor to *facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on*

the device in light of the teachings of Brown.

143. Brown discloses a system and method for deleting data, including personal data, from an electronic device.

A system and method for selectively securing data from unauthorized access on a client device storing a plurality of data types with reference to an authorization level indicated in a command. A command is received at a client device comprising an authorization level indicator. Based on at least one predefined rule, which may be implemented in an IT policy stored at the client device, each of the plurality of data types to be secured is determined, and then the data corresponding to those types is secured. The data may be secured by encrypting and/or deleting the data at the client device. The predefined rules associated with each authorization level may be configured by a user or administrator having an authorization level that exceeds the associated authorization level.

(Brown) APPL-1009, Abstract. *See also*, (Brown) APPL-1009, 1:15-18, 2:7-15, 11:65-13:14. FIG. 6 of Brown is illustrative of executing its wipe command:



(Brown) APPL-1009, FIG. 6

APPL-1009, 4:64-5:11, 11:65-66 (FIG. 6 is a flowchart of “execution of the wipe”

command on the client device[]”).

144. Brown describes that it may be desirable to delete all data on an electronic device.

Thus, it can be seen that there may be various categories of data stored at the client device 10, 100. Occasionally, it may be desirable to **delete data** at the client device 10, 100 to prevent its access by an unauthorized party. This deletion, which may comprise either the **overwriting of all** or **substantially all memory addresses in the data store 300, for example all but the addresses used to store the operating system 301 and PIM/messaging applications 305, may be accomplished through the invocation of a “wipe” command.**

(Brown) APPL-1009, 11:56-64. Brown’s “overwriting” data is deleting or wiping data. “The wiping process may also include repeated overwriting of ones, zeroes, or a random arrangement of ones and zeros over the data to be wiped.” (Brown) APPL-1009, 13:12-14. The teaching of overwriting **all** data of a client device is a teaching of overwriting the data of a biometric template and user credential in the client device of Kesanupalli. Benefits of wiping all data are readily recognizable for protection of all data for example when repurposing or retiring of the client device.

145. To the extent the Patent Owner argues the wiping must be

particularized to the recited elements, in addition to examples in Brown deleting all data from the device, Brown describes selective wiping of data. APPL-1009, Abstract, 2:18-35, 13:15-24. A POSITA would recognize that *the biometric template and the credential comprising the cryptographic key* of Kesanupalli are just the type of personal data that Brown suggests selectively wiping as the biometric template and credential are stored personal data related to the security functions of the device and Brown suggest its procedure applies to personal data such as security functions and encryption keys.

The data types may comprise at least one of an operating system, encryption and decryption keys, personal information management applications, messaging applications, e-mail data, short message service data, instant messaging data, multimedia message data, voicemail data, calendar data, address book data, or IT policies.

(Brown) APPL-1009, 3:12-18.

The data may further include applications, or data files created at the device or received by an authorized user at the device that are personal to the user, or that are used by the device for the management of data and/or security functions on the communication device.

(Brown) APPL-1009, 1:20-34.

146. Thus, a POSITA would have had reason to apply Brown's teachings to wipe the user's biometric template and the credential comprising the

cryptographic key of the at least one record stored at least in part in the storage on the device as it is a recognized desire to keep personal data protected from access by unauthorized or malicious users.

147. Further, Brown discloses a *processor* of the client device facilitates the *wiping*. See (Brown) APPL-1009, 4:7-44 (“a mobile client device for selectively securing data from unauthorized access of the client device...the device comprising a processor...the processor may be configured to secure the data by deleting the data corresponding to each of the plurality of data types thus determined in the memory...”); 9:12-38; 21:1-48; FIG. 2; 7:47-55. Therefore, it would have been obvious for Kesanupalli’s processor to facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device. Kesanupalli’s processor circuitry executing the sensor 204 has access to the record in the storage on the device to facilitate the wiping. The processor circuitry executing the PC 202 also facilitates in the wiping as it has communication with external services such as receive a command as in Brown FIG. 6.

148. Thus, Kesanupalli in view of Brown renders obvious this element.

k) [1.9] *a memory coupled to the processor and configured to provide the processor with instructions.*

149. Kesanupalli discloses *a memory coupled to the processor and configured to provide the processor with instructions.*

150. Kesanupalli's system includes a main memory, a *memory*.

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

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

152. Thus, Kesanupalli discloses this element.

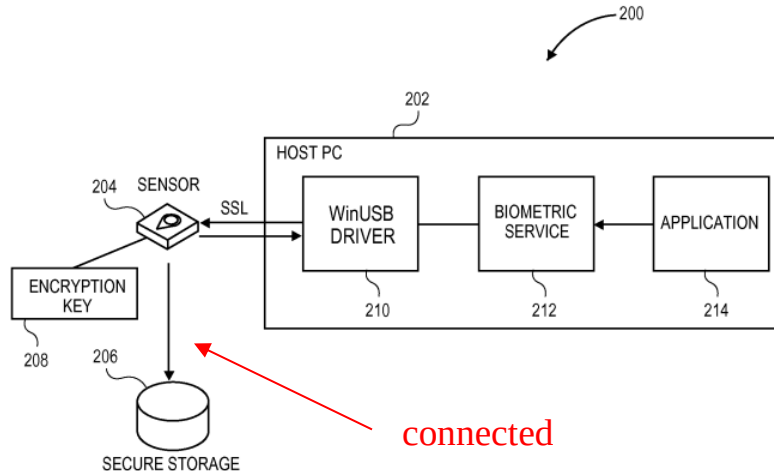
153. Therefore, Claim 1 is obvious over Kesanupalli and Brown.

5. Claim 2

[2.0] *The device recited in claim 1 wherein the storage is connected to a sensor.*

154. Kesanupalli and Brown render obvious claim 1, and Kesanupalli also discloses *the storage is connected to a sensor*.

155. Kesanupalli's secure storage 206 is connected to the sensor 204. See (Kesanupalli) APPL-1006, FIG. 2, 6:42-47.



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

156. Thus, Claim 2 is obvious over Kesanupalli and Brown.

6. Claim 3

[3.0] The device recited in claim 2 wherein the sensor comprises at least one of a camera and a fingerprint reader.

157. Kesanupalli and Brown render obvious claim 1, and Kesanupalli also discloses *the sensor comprises at least one of a camera and a fingerprint reader.*

158. Kesanupalli describes in an example the biometric input of a fingerprint is provided by a fingerprint sensor, which is a *fingerprint reader.*

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. Kesanupalli also describes that the biometric input can be a facial or eye characteristic. (Kesanupalli) APPL-1006, 2:30-35. A POSITA would understand that one typical way for capturing facial or eye characteristics inputs for authentication is a *camera*.

159. Thus, Claim 3 is obvious over Kesanupalli and Brown.

7. Claim 7

[7.0] *The device recited in claim 1 wherein facilitating wiping of the at least portion of the at least one record comprises facilitating remote wiping of the at least portion of the at least one record.*

160. Kesanupalli and Brown render obvious claim 1, and Kesanupalli in combination with Brown also teaches *facilitating wiping of the at least portion of the at least one record comprises facilitating remote wiping of the at least portion of the at least one record*.

161. Brown discloses facilitating remote wiping of data such as a record.

The client device may comprise a mobile communications device, and

the command may be received over the air, or received from input at the client device, or received as detection of a predetermined action, condition or trigger for the execution of the wipe command at the client device. In yet a further aspect, prior to receiving the command at the client device, the method may comprise defining, at a location remote from the client device, a plurality of predefined rules associated with an authorization level; and transmitting to the client device the plurality of predefined rules thus defined.

(Brown) APPL-1009, 2:63-3:6. FIG. 6 of Brown illustrates a “flowchart depicting a sequence of steps in the execution of the wipe command on the client device 10, 100. At step 500, the command is received at the client device 10, 100. ...

Invocation of the wipe command may be carried out at the server 40 by similar methods. ...” (Brown) APPL-1009, 11:65-12:21. “If the command is received from the server 40, in one embodiment it is received over the air; for example, a mobile communication device 100 may receive via the transceiver 411 (shown in FIG. 2) an incoming message from a remote location comprising a command at step 500...” (Brown) APPL-1009, 12:28-35. FIG. 1 of Brown illustrates server 40 is remote from device 100.

162. The ’138 patent does not define “remote wiping,” however under the heading of “Remote wiping,” the ’138 patent provides an example of “self-wipes.”

('138 patent) APPL-1001, 8:35-38. To the extent the Patent Owner argues remote wiping is self-wiping, Brown also discloses this use of its policies. Brown similarly teaches wiping where actions such as entering a password incorrectly, the wiping command self-executes. (Brown) APPL-1009, 12:6-12. See also the analysis in Claim 8 below.

163. Therefore, Claim 7 is obvious in light of Kesanupalli and Brown.

8. Claim 8

[8.0] *The device recited in claim 1 wherein the at least portion of the at least one record is automatically wiped based at least in part on a policy.*

164. Kesanupalli and Brown render obvious claim 1, and Kesanupalli in combination with Brown also teaches *at least portion of the at least one record is automatically wiped based at least in part on a policy.*

165. Brown discloses providing a policy, which it refers to as an IT policy, which is stored in the client device and defines rules for the wiping.

A system and method for selectively securing data from unauthorized access on a client device storing a plurality of data types with reference to an authorization level indicated in a command. A command is received at a client device comprising an authorization level indicator. Based on at least one predefined rule, which may be implemented in an IT policy stored at the client device, each of the plurality of data types to be secured is determined, and then the data corresponding to those

types is secured. The data may be secured by encrypting and/or deleting the data at the client device. The predefined rules associated with each authorization level may be configured by a user or administrator having an authorization level that exceeds the associated authorization level.

(Brown) APPL-1009, Abstract. *See also*, (Brown) APPL-1009, 16:40-45, 1:56-59, 11:22-31, FIG. 3 including IT policies 315, FIG. 4a, FIG. 4b. The policy may include various predefined rules related to a wipe including which data is *automatically* wiped on the wipe command:

In a more robust implementation such as that illustrated in FIG. 4a, the IT policy may comprise rules relating to the authorization level required to enable a wipe of the PIM/message data (PIMMessageDataWipeMinLevel), user-entered data (UserDataWipeMinLevel), IT policy (ITPolicyWipeMinLevel), third-party applications (ThirdPartyAppWipeMinLevel), PIM/message applications (PIMMessageAppWipeMinLevel), or key data (KeyDataWipeMinLevel).

(Brown) APPL-1009, 14:20-28. *See also*, (Brown) APPL-1009, 15:46-49, 16:40-45, FIGS. 8a, 8b. As discussed above with reference to Claim 1, it would have been obvious to wipe the at least portion of the at least one record including the personal data of the biometric template and user credential to enhance the security

of that data. For the same reasons it would have been obvious to designate this data in the policy as being data that is to be wiped, and thus is automatically wiped based at least in part on the policy.

166. Brown also describes predefined rules for predetermined actions, which are themselves a *policy*, that trigger execution automatic wiping of the client device. In an example, Brown describes implementing a policy of an automatic wiping if a predetermined action of entering a password incorrectly too many times occurs.

The wipe command may alternatively be invoked by a user or administrator deliberately or accidentally engaging in a predetermined action at the client device 10, 100, such as entering a password incorrectly for a predetermined number of times, resulting in receipt at the client device 10, 100 of the incorrect password for the predetermined number of times, or by carrying out another predetermined action or entering into a predetermined condition that triggers the execution of the wipe command by the client device 10, 100.

(Brown) APPL-1009, 12:6-12.

167. Therefore, Claim 8 is obvious in light of Kesanupalli and Brown.

9. Claim 12

[12.0] *The device recited in claim 1, wherein the storage comprises a secure storage.*

168. Kesanupalli and Brown in combination teach all elements of claim 1, and Kesanupalli further discloses *the storage comprises a secure storage*.

169. 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.")

170. A *secure storage* is one that is protected from unauthorized use. By describing its storage as "secure storage," a POSITA would understand Kesanupalli to be providing a secure storage area that is protected from unauthorized use. As illustrated by Kesanupalli's FIG. 2, use of the secure storage 206 is controlled by the sensor 204, and is not directly accessible by others (e.g., application 214 executing on the Host PC 202), for example, the user credential in the storage cannot be accessed except by the sensor 204 when verifying a match of biometric input as discussed in limitation [1.5A]. Therefore, the secure storage 206 is *secure storage*.

171. Thus, Claim 12 is obvious over Kesanupalli and Brown.

10. Claims 13– 15, 19, and 24

172. The limitations of independent Claim 13, except the preamble of the claim are substantively identical to limitations of claims already addressed above,

as correlated in the table below:

Claim 13 Limitation	Corresponding Claim Limitation of Claim 1 illustrating the substantially similar limitation of Claim 25 is disclosed in Kesanupalli and/or Brown
[13.1a] <i>based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate access of at least one record stored at least in part in a storage on the device, wherein the storage on the device is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device;</i>	[1.1], [1.2], [1.3]
[13.2] <i>wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key;</i>	[1.4]
[13.3a] <i>in response to determining a match between a biometric input and the biometric template, retrieving, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature,</i>	[1.5A]
[13.3b] <i>wherein the biometric input is received subsequent to presenting of a prompt, wherein</i>	[1.5B]

<i>the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;</i>	
<i>[13.4] establishing a connection with the external resource;</i>	<i>[1.6]</i>
<i>[13.5] facilitating a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and</i>	<i>[1.7]</i>
<i>[13.6] facilitating, by the processor on the device, wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device.</i>	<i>[1.8]</i>

[13.0] A method, comprising:

173. To the extent the preamble is limiting, Kesanupalli and Brown disclose it. The citations to Kesanupalli and Brown 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. ...”); (Brown) APPL-1009, Abstract (“method for selectively securing data from unauthorized access on a client device storing a plurality of data types...”), 1:55-56 (“FIG. 6 is a flowchart of a method for processing a wipe command a communication device.”).

174. Thus, Claim 13 is obvious in light of Kesanupalli and Brown.

175. Dependent Claims 14–15, 19, and 24 are substantively identical to claims already addressed above, as correlated in the table below. The combination of Kesanupalli and Brown renders obvious these claim for the same reasons discussed above with respect to Claim 13 and the corresponding claims in of the table.

Claim	Corresponding Claim analyzed above illustrating the elements are disclosed in Kesanupalli and/or Brown
[14]	[2]
[15]	[3]
[19] ¹³	[7]
[24]	[12]

11. Claim 25

176. The limitations of Claim 25, except the preamble, are substantively identical to limitations of Claim 1 already addressed above, as correlated in the table below:

Claim 25 Limitation	Corresponding Claim Limitation illustrating Claim 25 is disclosed in Kesanupalli and/or Brown
---------------------	---

¹³ Claim 19 has a preamble of a “method” but purports to depend from Claim 12, which is a device claim. Whether Claim 19 is directed to a method such as claim 13, or a device such as claims 1 and 12, it is obvious over Kesanupalli and Brown for the reasons discussed in Claim 7.

[25.1] <i>based at least in part on a request from a user to access an external resource, using a processor on a device to facilitate access of at least one record stored at least in part in a storage on the device, wherein the storage on the device is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device;</i>	[1.1], [1.2], [1.3]
[25.2] <i>wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises: a biometric template; and a credential comprising a cryptographic key;</i>	[1.4]
[25.3a] <i>in response to determining a match between a biometric input and the biometric template, retrieving, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature,</i>	[1.5A]
[23.3b] <i>wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;</i>	[1.5B]
[24.4] <i>establishing a connection with the external resource;</i>	[1.6]
[25.5] <i>facilitating a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and</i>	[1.7]
[25.6] <i>facilitating, by the processor on the device, wiping of both the biometric template and the</i>	[1.8]

<i>credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device.</i>	
---	--

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

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

178. The citations to Kesanupalli and Brown above apply to a *device* 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. See also, (Brown) APPL-1009, 19:17-24 (“The systems and methods data may be stored in one or more data stores. The data stores can be of many different types of storage devices and programming constructs, such as RAM, ROM, flash memory, programming data structures, programming variables, etc. It is noted that data structures describe formats for use in organizing and storing data in databases, programs, memory, or other computer-readable media for use by a computer program.”)

179. Thus, Claim 25 is obvious over Kesanupalli and Brown.

B. Ground 2: Claims 10 and 22 are obvious under 35 U.S.C. § 103 over Kesanupalli in view of Brown and in further view of Cheng.

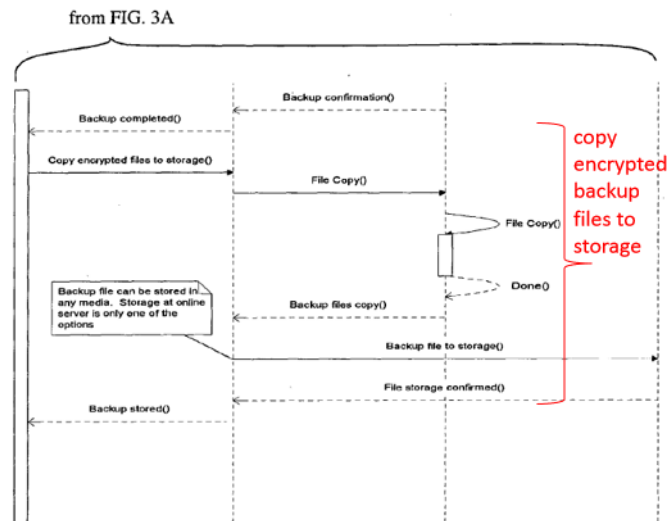
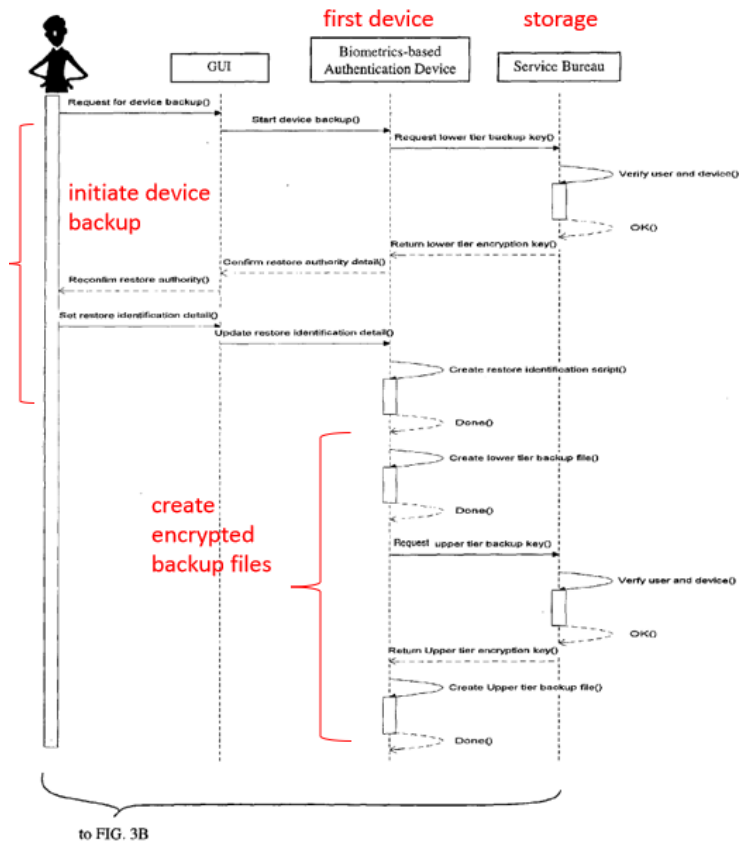
1. Summary of Cheng

180. 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).

181. 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].

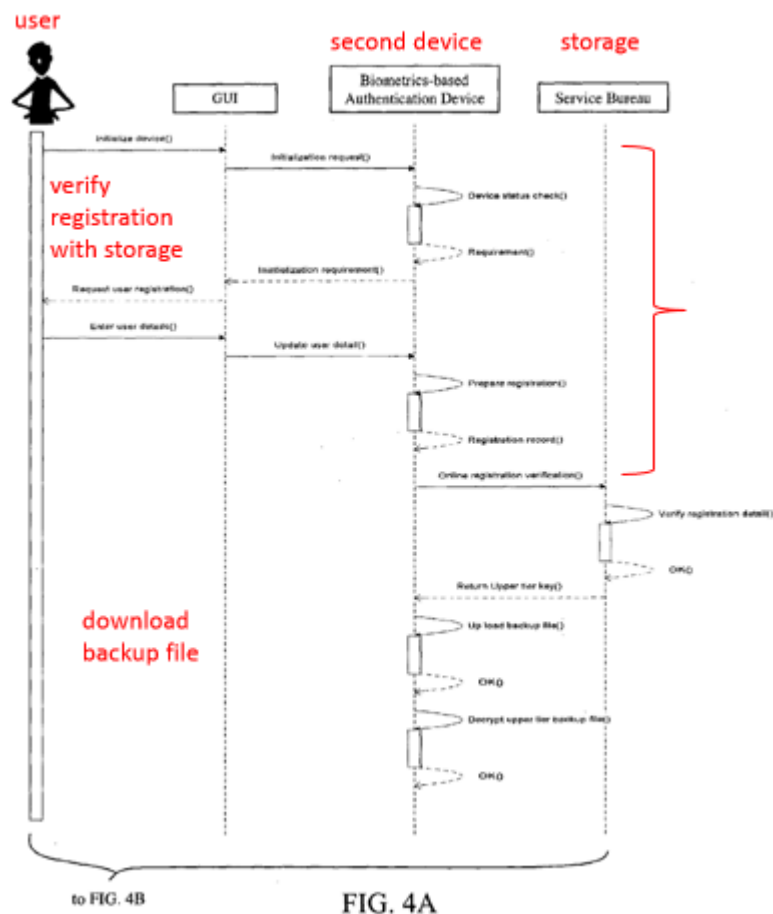
182. Cheng teaches performing a secure backup of this data to avoid costs of registering a new device from scratch should a first device containing the data be lost or stolen. *See* (Cheng) APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng’s FIGS. 3A-3B where a backup of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

service bureau 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].



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

183. 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. (Cheng) APPL-1008, [0044] – [0050], FIGS. 4A-4C.



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

2. Reasons to Combine Kesanupalli, Brown and Cheng

184. A POSITA would have been motivated to apply Cheng's teachings of backing up data from storage of an electronic device to a remote entity such as the device used in Kesanupalli that stores biometric information associated with a user and credentials for user authentication to resources such as websites.

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 replacing a lost or stolen device.

185. First, like Kesanupalli, Brown and the '138 patent as discussed above, Cheng is also analogous art and all are in the same field of endeavor such as security arrangements and procedures for protecting data in computer systems. *See, supra*, (Cheng) APPL-1008, [0002], [0003]. Cheng is directed to handling of personal data of a computer system in a secure manner that protects the data from trespassers and security attacks. (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."). Like Kesanupalli, Brown and the '138 patent, Cheng also similarly directed to protection of a user's authentication data. (Cheng) APPL-1008, [0004],

[0007] (“The present invention provides new ways to **securely backup** and restore a user’s **authentication information**, electronic identity and any data associated therewith, without comprising the security thereof.”); (Kesanupalli) APPL-1006, FIG. 2, Abstract; (Brown) APPL-1009, 1:15-2:8; (’138 Patent) APPL-1001, 2:40-59. And Cheng relies on “enabling technologies” that are just like those of Kesanupalli, Brown and the ’138 Patent as suggested by their field of search classification discussed above. (Cheng) APPL-1008, [0007] (“Enabling technologies include biometrics, authentication, cryptography, and encryption/decryption.”)

186. Second, a POSITA would have been motivated to employ Cheng’s backup procedure in connection with Kesanupalli’s secure authorization system and methods and Brown’s wiping technique because a POSITA would recognize that while Kesanupalli as modified by Brown has a benefit of wiping data to preserve security as discussed above, wiping data necessitates recreating of the wiped data when the user procures a second (*e.g.*, replacement) device. As the stored biometric information and credentials are deleted when implementing Brown’s wiping procedure, a POSITA would have understood that this deletion of the user’s personal data raises cost and inconvenience to the user as she no longer has access to her data. Such a problem would also have been reasonably pertinent to the inventors of the challenged patent. (’138 patent) APPL-1001, 8:38-41 (“user

data can be frequently backed up to the cloud storage, and recovered from this...[and] inconvenience to the user will be minimized.”). 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]. 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. (Cheng) APPL-1008, [0007]. Thus, not only were Kesanupalli, Brown, Cheng and the '138 patent in the same field of endeavor, but Cheng would have been reasonably pertinent to a problem faced by the inventors of the '138 patent and pertinent to known risks of loss of devices and data such that a POSITA have been motivated to address the preservation of data in the Kesanupalli-Brown

combination by implementing the teachings of Cheng. *See* (Kesanupalli) APPL-1006, 10:13-18.

187. To address costs of this risk of loss of device and/or data, Cheng teaches backing up of the data of the electronic device including biometric information and secret keys. (Cheng) APPL-1008, [0007] – [0009]. A POSITA would benefit from providing Cheng’s teachings to the system/method/ computer program product of Kesanupalli in view of Brown in order to avoid the “cost and inconvenience” of recreating the data wiped from an electronic device when the data is desired to be provided on a new or replacement device. *See* (Cheng) APPL-1008, [0006] - [0007]. The user would continue to desire access to the websites with which she had enrolled, and thus, desire to have continued access to the credential (and biometric template) in order to obtain that access. Simply put, backing up the data avoids recreating the enrollment of FIG. 7 of Kesanupalli. Moreover, a POSITA would have recognized a desire in the market of electronic devices for secure data to be capable of being backed up long before the ’138 patent.¹⁴ From the first introduction of electronic data itself, a POSITA recognized a user’s desire to backup that data to avoid its loss. A POSITA would appreciate a

¹⁴ *See, e.g.*, APPL-1020

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

desire of the user to backup secure data such as personal data, which can be particular target data for wiping techniques discussed above in Brown. Cheng specifically recognizes that backup is especially important to combine with security practices that direct for wiping data. See (Cheng) APPL-1008, [0006].

188. Finally, POSITA would have had reasonable expectations of success in adding a backup procedure such as taught by Cheng in a biometric authentication system such as taught by Kesanupalli in view of Brown, as Cheng is similarly directed to improving security of personal information. (Cheng) APPL-1008, [0022]. Adding a backup procedure 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 technique is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices as in particular as enhanced by the teachings of Brown.

3. Claim 10

[10.0] *The device recited in claim 1 wherein the at least portion of the at least one record is backed up to a remote entity.*

189. Kesanupalli and Brown in combination teach claim 1, and Cheng discloses *the at least portion of the at least one record is backed up to a remote entity.*

190. First, Cheng discloses performing a back-up of data to a remote entity

such as an internet-based storage service.

An exemplary backup process is illustrated in FIGS. 3A-3B. The storage means could be, for instance, an online proprietary or Internet-based storage service, a remote server, a floppy disk, a hard drive, a data drive, a CD-ROM, an optical storage means, a removable disk, a smart card, a memory storage device or any other storage media capable of storing data.

(Cheng) APPL-1008, [0029]. *See also*, (Cheng) APPL-1008, FIGS. 3A, 3B.

[0023] – [0028] describes a method culminating in “(e) storing the encrypted lower tier backup file and the encrypted upper tier backup file on a storage means.” An online proprietary or internet-based storage service is a *remote entity*.

191. A POSITA would have applied Cheng’s teachings of its backup process to a remote entity to the data of Kesanupalli’s device and in particular the *record*. This is because not only does Cheng generally suggest the back up of data of an electronic device generally, but Cheng also provides specific examples of data that is backed up including a private key, which is just like the cryptographic key of the record of Kesanupalli discussed above, and biometric data. “In a preferred embodiment, the lower tier authentication data include private keys, certificates, and other data held within the device. In this embodiment, the upper tier authentication data include the user’s biometrics information.” (Cheng) APPL-1008, [0030]. *See also*, (Cheng) APPL-1008, [0008] (“The lower tier data contain encrypted electronic identity such as private keys and associated certificates. The

upper tier data contain the encrypted lower tier data, restore validation script, and biometrics data.”), [0015], FIG. 1, claim 2.

192. Thus, a POSITA would have been motivated to use Cheng’s back up method to back up, to a remote entity, *the at least one record* of Kesanupalli as discussed in the reasons to combine above including to recognize the benefits of, “[i]n the event of loss, damage, or destruction of the device,” avoiding cost and inconvenience of the user to create and register new templates and keys when erased as taught by Brown’s security procedures applied to Kesanupalli. See, (Cheng) APPL-1008, [0006].

193. Thus, Claim 10 is obvious over Kesanupalli in view of Brown and Cheng.

4. Claim 22

[22.0] *The method of claim 13 wherein the at least portion of the at least one record is backed up to a remote entity.*

194. For the same reasons as discussed with respect to Claims 10 and 13, Claim 22 is rendered obvious by Kesanupalli in view of Brown and Cheng.

C. Ground 3: Claims 11 and 23 are obvious under 35 U.S.C. § 103 over Kesanupalli in view of Brown and in further view of Challenger.

1. Summary of Challenger

195. Challenger “relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement

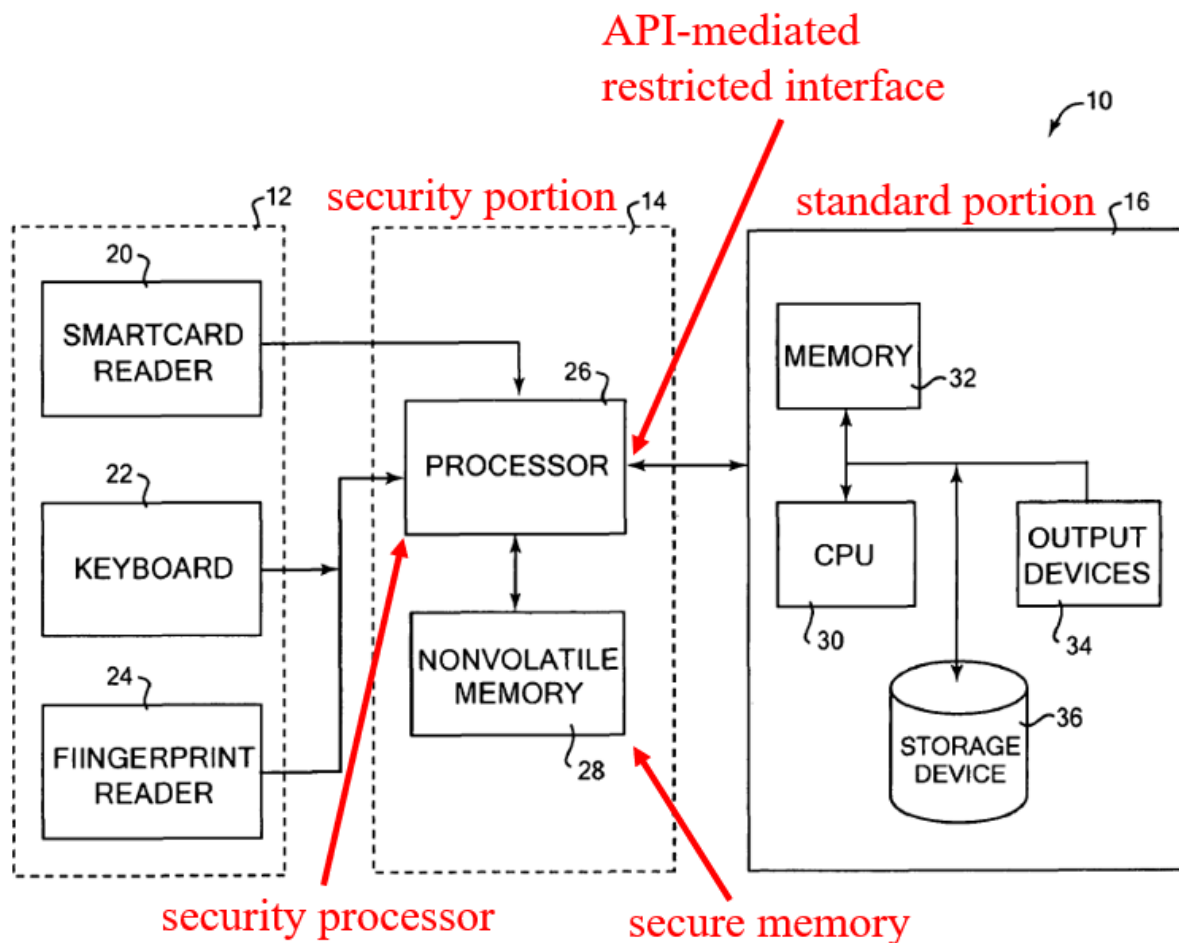
security features.” (Challener) APPL-1007, 1:7-9, 3:24-26. Challener illustrates a system 10¹⁵ (*e.g.*, computer or electronic device) with a system architecture suitable for securing data and functions of system 10 from unauthorized access and manipulation. (Challener) APPL-1007, 3:48-56. In particular, 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, 3:44-57. 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.

196. Broadly speaking, TPMs provide a platform for performing trusted computing features. 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. TPMs offer a variety of features, including a random number generation, for secure generation of cryptographic keys, and the use of keys, *e.g.*, to signing and signature verification, and encryption and decryption.

¹⁵ “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.

(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. One example of such the API-mediated interface in a TPM architecture is “[t]he 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.”¹⁶ In other words, a component can only access the TPM if it is in a “trusted” (i.e., restricted) configuration.

¹⁶ APPL-1017, https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf



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

197. 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 API-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, Brown and Challener

198. 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 Brown’s selectively wiping of sensitive data 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 Brown’s techniques.

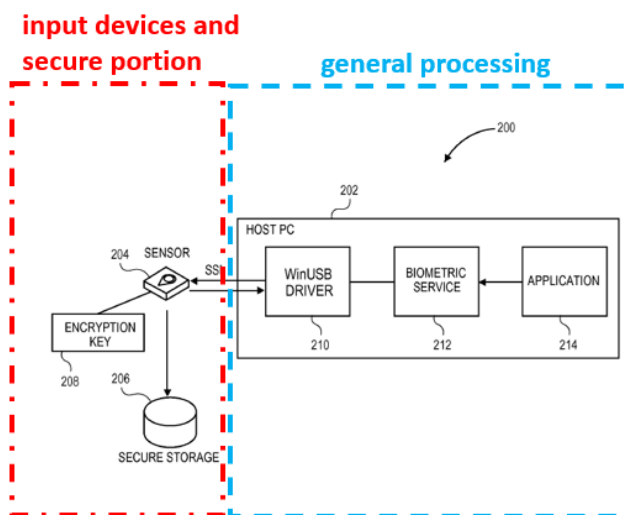
199. First, Challener, Kesanupalli, Brown and the ’138 patent are analogous art and are all in the same field of endeavor—namely, information security, and more particularly, security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. (Challener) 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*, Section VIII.A.3 (reasons to combine Kesanupalli and Brown). Moreover, Challenger bears the very the IPC subclass—CPC/IPC G0F6 21 as discussed above relative to Kesanupalli, Brown and the ’138 patent. (Challener) APPL-1007, (51); *see also*, , Section VIII.A.3.

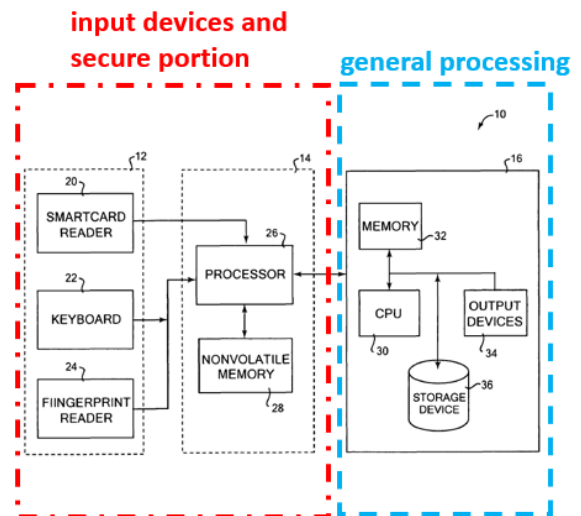
200. Second, a POSITA would have been motivated to apply Challenger’s teachings of a standards-based TPM architecture as an implementation framework for Kesanupalli’s biometric security techniques given the support that a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided. (Challener) APPL-1007, 1:18-31 (summarizing typical TPM functions and APIs). Indeed, Challenger’s description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data, *e.g.*, “secure hash values and ... keys,” *and* fingerprint reader 24 behind a security processor 26 that “implements the particular security features and functions (*e.g.*, API functions, algorithms)” in a system that includes secure and non-secure portions. (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 provide compatibility and

robustness, and therefore and therefore engender trust amongst users and customers.¹⁷

201. 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.



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Note 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

¹⁷ See, e.g., APPL-1016, <https://www.iso.org/standard/50970.html>

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.

202. Finally, a POSITA would have had reasonable expectations of success in implementing Kesanupalli's a biometric authentication techniques and in applying Brown's wipe features to a sensitive data in secure storage given that Challenger'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 supra* VI.E. In contrast, Kesanupalli's architecture, which while it shares features with a TPM-based system is as Challenger states one of many different techniques used to secure information and does not enjoy the recognized security 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 11

[11.0] *The device recited in claim 1, wherein the interface comprises a restricted interface.*

203. Claim 1, from which claim 11 depends, is obvious over Kesanupalli in

view of Brown as demonstrated in Ground 1. *See above.* Kesanupalli and Challener teach this additional element.

204. As discussed above, one deploying the security functions of Kesanupalli's sensor 204 would have been motivated to implement those functions on Challener's TPM-based security architecture using specialized security processing circuitry such as illustrated by Challener's security processor 26. *See* secure portion 16 and its processor 26 of Challener corresponding to the sensor 204 of Kesanupalli above. (Challener) APPL-1007, 4:9-24, FIG. 1. As detailed below, Challener's interfaces with and within the secure portion of its architecture are restricted interfaces.

205. In particular, one would have had reason to implement the functionality of sensor 204 of Kesanupalli using the secure processor 26 and Kesanupalli's secure memory 206 using Challener's corresponding secure memory, non-volatile memory 29. (Challener) APPL-1007, 4:57-65 ("memory 28 is a secure memory which cannot be easily tampered with to read its data contents. In some embodiments, the nonvolatile memory 28 can be included on the same integrated circuit chip [] of the processor 26.") A "*restricted interface*" is an interface that limits accessibility. *See* Section VII.B. A POSITA would have recognized that secure processor 26 communicates with its on-chip secure memory 28 using a *restricted interface* because the interface therebetween limits secure

storage access to just security processor 26. APPL-1007, FIG. 1. Other components such as those of the standard or general portion do not access the memory 28 except through the processor 26. As indicated above, the security architecture of Challenger implements a nonvolatile memory 28 integrated with and physically connected to the secure processor 26 to hold secure data. Challenger 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. A POSITA would also recognize that Challenger teaches that the memory may be integrated with the processor. (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)”).

206. As discussed in Section VI., the ’138 patent discusses the restricted interface only in terms of an API. To the extent that the Patent Owner argues the configuration of Challenger discussed above is an insufficiently restricted interface, Challenger also teaches API-mediated interfaces. Based on the ’138 patent’s limited description, POSITA would understand “*restricted interface*” to at least include an API that limits accessibility to a secure storage, a fingerprint sensor, or dedicated processor. See Section VI. In particular, Kesanupalli (implemented using Challenger’s TPM framework for secure systems), communication between the security portion (sensor 204 and memory 206) and the standard portion (PC

202) occurs through an API-mediated interface, a *restricted interface*, as detailed below.

207. TPM-based implementations, including Challenger'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 that restricts access to the TPM (secure processor) and its secure memory by programs running on a general processor in a standard (non-secure) portion of a system such that the general processor programs are limited from access to the security-related operations and stored data, such as key and credential management, secure storage, encryption, decryption and digital signatures that are in a secure portion of the system. See VI.E. See also, (Challener) APPL-1007, 4:3-15 discussing controlling "access."

208. Challenger further discloses a restricted interface (in the form of an API) relative to secure processor 26, which implements a TPM-based security architecture that includes API functions for its communication with other components – including the general processor 30. (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. Simply put, an API is software

that defines how two components, for example processor 26 and general processor 30 communicate with one another. Moreover, because the API implemented by processor 26 is an access limiting interface through which general processor 30 must interface, it also provides the interface—indeed the restricted interface—for any communications between functions executing on general processor 30 and the secure storage.

209. More generally, a TPM-based API, such as provided by Challenger's processor 26, provides restrictions by the way of a set of rules or restrictions that POSITA would understand are defined by the TPM standard for access to the security portion 16 of the system including its secure storage. Such restrictions limit access and thereby protect the functions and data in the security portion of a TPM-based security architecture from being misused by an untrusted or malicious program. Thus, this API interface provided by the TPM is a *restricted interface*, whether the term is formally construed or merely understood in accord with plain and ordinary meaning. See above at VI.E.

210. Thus, Claim 11 is also obvious over Kesanupalli and Brown further in view of Challenger.

4. Claim 23

[23.0] *The method of claim 13, wherein the interface comprises a restricted interface.*

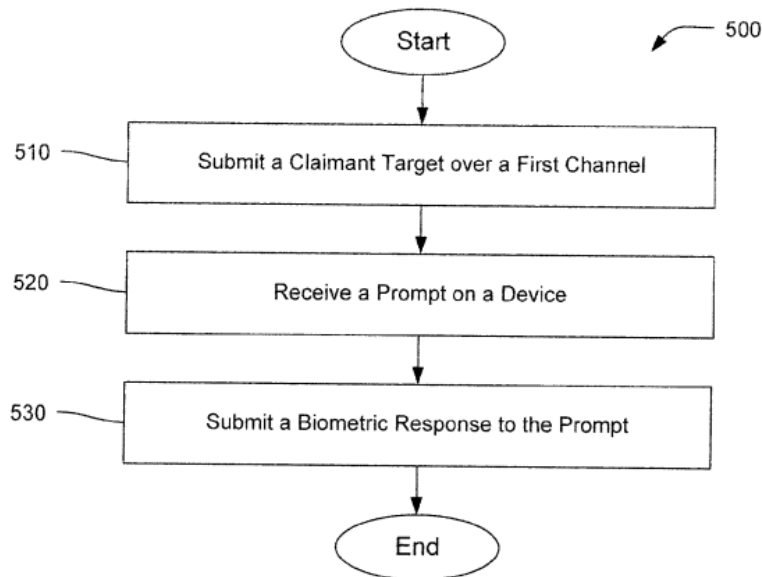
211. For the same reasons as discussed with respect to Claim 11 and due to

Claim 23's dependency on corresponding Claim 13, Claim 23 is rendered obvious either by Kesanupalli and Brown (alone) or by Kesanupalli and Brown further in view of Challener.

D. Ground 4: Claims 5 and 17 are obvious under 35 U.S.C. §103(a) over Kesanupalli and Brown further in view of Headley.

1. Headley

212. Headley is entitled "User authentication for social networks" and provides "[v]erification can be performed, for example, by reference to biometric templates stored during the user enrollment process. The biometric templates can also be used to authenticate users logging into the social network to prevent user impersonation." (Headley) APPL-1010, (54), Abstract. Headley recognizes the need for authentication of users to avoid individuals misrepresenting themselves to gain unauthorized access to an account for illegitimate use. (Headley) APPL-1010, 1:32-45. In response to this, Headley describes methods for a user's initial enrollment to an external service including providing biometric samples such as a fingerprint, and then after enrollment, a system prompts a person seeking to the service to provide a biometric response for authentication. (Headley) APPL-1010, 3:41-57. Headley teaches that "[t]he prompt can be provided visually, **aurally** or in combination." (Headley) APPL-1010, 7:48-50.



(Headley) APPL-1010, FIG. 5

2. Reasons to Combine Kesanupalli, Brown and Headley

213. POSITA would have been motivated to apply Headley’s teachings of providing a prompt aurally to elicit a user’s biometric input in Kesanupalli’s device. Kesanupalli’s device providing a prompt for biometric input visually, with Headley’s teachings with respect to providing a prompt aurally would produce the obvious, beneficial, and predictable results of increasing the robustness of the requesting prompt to the user. Simply put, presenting a user a request for information (e.g., a biometric input) in two different ways provides efficiencies to the user in recognizing the need for input.

214. First, like Kesanupalli, Brown and the ’138 patent as discussed above, Headley is also analogous art and in the same field of endeavor—namely, security

arrangements and procedures for protecting data in computer systems. *See supra* Section VIII.A.3 (**Error! Reference source not found.**); (Headley) APPL-1010, 3:17-40. Headley lists the same classification search - CPC/IPC G0F6 21. *See supra* Section VIII.A.3 (**Error! Reference source not found.**); (Headley) APPL-1010, (51). Further, Headley describes the same methods of biometric authentication - initial enrollment with an external service user account that includes providing a biometric input, and subsequent authentication of a user by providing a biometric input in response to a prompt. *See* (Headley) APPL-1010, (57); ('105 patent) APPL-1001, 4:41-49, 5:10-19.

215. Second, POSITA would have been motivated to employ Headley's presentation of prompts in connection with Kesanupalli's secure authorization system and methods including Brown's wiping technique because POSITA would recognize that while Kesanupalli-Brown has a *visual* prompt to provide biometric data additionally introducing a different and/or an additional manner of presenting the prompt allows a system to reach more users and/or increase a convenience to a user in recognizing a prompt.

216. Finally, POSITA would have had reasonable expectations of success in adding an aural prompt such as taught by Headley in a biometric authentication system such as taught by Kesanupalli in view of Brown, as Headley is similarly directed to improving security of a user's data through biometric authentication

procedures. Indeed, an aural prompt is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli's system and devices as enhanced by the teachings of Brown.

3. Claim 5

[5.0] *The device recited in claim 1 wherein the prompt is aurally presented.*

217. As explained above, Kesanupalli and Brown render obvious claim 1. Kesanupalli, Brown and Headley render obvious the further limitation of claim 5. Headley describes providing a user's device, which may include a cell phone, smart phone, PC etc., which presents a prompt for biometric input where the prompt is presented visually, aurally, or a combination thereof. Headley describes the device is "able to receive and render a prompt from the authentication system 110 and/or transmit a response thereto. The prompt can be provided by the second device 140 **visually, aurally, or in combination**, for example. For instance, the prompt can be displayed as a text message, a verbal command or cue, an audio clip, a video clip, etc. In some instances, the second device 140 can be used by the claimant to provide the biometric response to the authentication system 110." APPL-1010 (Headley) 7:39-58. Thus, a POSITA would have been motivated to use Headley's presentation of a prompt presenting a prompt visually and aurally in the device of Kesanupalli as discussed in the reasons to combine above including

to recognize the benefits of presenting a prompt in more than one manner. If Patent Owner argues that the claim requires only aural presentation, Headley also teaches aural as an alternative to visual presentation.

218. Thus, claim 5 is obvious over Kesanupalli, Brown and Headley.

4. Claim 17

[17.0] *The method of claim 13 wherein the prompt is aurally presented.*

219. As explained above, Kesanupalli and Brown render obvious claim 13. Kesanupalli, Brown and Headley render obvious the further limitation of claim 17. In particular, for the same reasons as discussed with respect to claims 5 and 13, claim 17 is rendered obvious by Kesanupalli, Brown and Headley.

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