

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,

Petitioner

v.

CARBYNE BIOMETRICS, LLC,

Patent Owner

IPR2024-00332

U.S. Patent No. 10,929,512

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES	1
	A. Real Party-in-Interest	1
	B. Related Matters.....	1
	C. Lead and Back-up Counsel and Service Information	2
III.	GROUND FOR STANDING.....	3
IV.	THE '512 PATENT.....	3
	A. Summary of the '512 patent.....	3
	B. Prosecution History	5
V.	LEVEL OF ORDINARY SKILL IN THE ART.....	6
VI.	CLAIM CONSTRUCTION	6
	A. “restricted interface”.....	7
VII.	REQUESTED RELIEF	9
VIII.	OVERVIEW OF CHALLENGES	9
	A. Challenged Claims	9
	B. Statutory Grounds for Challenges.....	9
IX.	IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE..	10
	A. Ground 1: Claims 1-6, 10-16 and 20-21 are Rendered Obvious under §103(a) over Kesanupalli, Challener and Cheng	10
	1. Kesanupalli.....	10
	2. Challener	12
	3. Cheng	15
	4. Overview of Kesanupalli and Challener Combination.....	18
	5. Reasons to Combine Kesanupalli and Challener	21
	6. Reasons to Combine Kesanupalli, Challener and Cheng	24
	7. Claim 1	27
	8. Claim 2	60

9.	Claim 3	61
10.	Claim 4	63
11.	Claim 5	64
12.	Claim 6	65
13.	Claim 10	66
14.	Claims 11–16 and 20	67
15.	Claim 21	69
X.	DISCRETIONARY DENIAL IS NOT WARRANTED	72
A.	The <i>Fintiv</i> factors favor institution.	72
B.	The Board should not deny under General Plastic	74
C.	<i>Advanced Bionics</i> Test Favors Institution.	76
XI.	CONCLUSION	79
XII.	CERTIFICATE OF WORD COUNT	80
	CERTIFICATE OF SERVICE	81

PETITIONER’S EXHIBIT LIST

January 19, 2024

APPL-1001	U.S. Patent No. 10,529,512 to Jakobsson (“’512 patent”)
APPL-1002	Prosecution History of the ’512 patent
APPL-1003	Declaration of Dr. Patrick McDaniel
APPL-1004	<i>Curriculum Vitae</i> of Dr. Patrick McDaniel
APPL-1005	Reserved
APPL-1006	U.S. Patent No. 8,799,666 (“Kesanupalli”)
APPL-1007	U.S. Patent No. 8,099,789 (“Challener”)
APPL-1008	U.S. Patent Publication No. 2004/0117636 (“Cheng”)
APPL-1009	U.S. Patent No. 9,652,629 (“Brown”)
APPL-1010	Reserved
APPL-1011	Reserved
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
APPL-1016	ISO/IEC 11889-1:2009 Information technology Trusted Platform Module Part 1: Overview at https://www.iso.org/standard/50970.html
APPL-1017	TPM Main Part 3 Commands Specification Version 1.2 1 March 2011 at https://trustedcomputinggroup.org/wp-content/uploads/TPM-Main-Part-3-Commands_v1.2_rev116_01032011.pdf

APPL-1018	Infineon White Paper, <i>TPM Key Backup and Recovery For Trusted Platforms</i> , https://www.infineon.com/dgdl/Infineon-TPM_Key_Backup_and_Recovery-AP-v01_00-EN.pdf?fileId=db3a304412b407950112b41656d7203a (2006)
APPL-1019	Computer Dictionary, Second Edition, entry “data record” (1994)
APPL-1020	How to Restore Your Data After a Hard Drive Crash, Glenn Derene, Aug 4, 2011 at https://www.popularmechanics.com/technology/gadgets/how-to/a6819/how-to-restore-your-data-after-a-hard-drive-crash/
APPL-1021	U.S. Patent Application No. 2007/0100913 to Sumner et al.
APPL-1022	U.S. Patent Application No. 2008/0104416 to Challenger et al. (“Challenger’s PG-PUB”)
APPL-1023	RFC2818, HTTP Over TLS (May 2000)
APPL-1024	Trusted Computing Group, Enterprise Security: Putting the TPM to Work, 2008 at https://trustedcomputinggroup.org/wp-content/uploads/TPM-Applications-Whitepaper.pdf (retrieved Jan. 2, 2024)
APPL-1025	Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation, (June 21, 2022) (“Director Memo)
APPL-1026	Preliminary Constructions, <i>Carbyne Biometrics v. Apple, Inc.</i> , 1:23-cv-00324 (December 11, 2023)
APPL-1027	United States District Courts—National Judicial Caseload Profile (September 30, 2023), https://www.uscourts.gov/statistics/table/na/federal-court-management-statistics/2023/09/30 (retrieved Dec. 14, 2023)
APPL-1028	Scheduling Order, <i>Carbyne Biometrics, LLC v. Apple Inc.</i> , WDTX-1:23-cv-00324 (July 14, 2023)

I. INTRODUCTION

U.S. Patent No. 10,929,512 (the “’512 patent”) relates to “Authentication Translation” where a request to access a resource and an authentication input is received, and in response, “a previously stored credential associated with the resource is accessed” and provided to the resource. APPL-1001, Title, Abstract. Apple Inc. (“Petitioner” or “Apple”) respectfully requests the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-6, 10-16, and 20-21 (“Challenged Claims”) of the ’512 patent.

II. MANDATORY NOTICES

A. Real Party-in-Interest

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

B. Related Matters

Pursuant to 37 C.F.R. §42.8(b)(2), the ’512 patent is or was involved in the following matters, which may affect, or be affected by, this proceeding:

- *Carbyne Biometrics, LLC v. Apple Inc.*, 1:23-cv-00324 (WDTX), filed March 24, 2023 (Pending) (“Parallel District Court Proceeding”)
- *RightQuestion, LLC v. Samsung Electronics Co., Ltd. et al.*, 2:21-cv-00238 (EDTX), filed June 29, 2021 (terminated July 22, 2022)

- *Samsung Electronics Co., Ltd. et al v. RightQuestion, LLC*, IPR2022-00251 (PTAB), filed December 1, 2021 (terminated June 9, 2022) (“Samsung ’512 Patent IPR”)

Apple is not aware of any disclaimers, reexamination certificates or other IPR petitions addressing the ’512 patent; however, the following matter involved a related application and may affect this proceeding:

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

C. Lead and Back-up Counsel and Service Information

Lead Counsel

David W. O’Brien	Phone: (512) 867-8457
HAYNES AND BOONE, LLP	Fax: (214) 200-0853
2801 N. Harwood St., Suite 2300	david.obrien.ipr@haynesboone.com
Dallas, TX 75201	USPTO Reg. No. 40,107

Back-up Counsel

Kelly Gehrke Lyle	Phone: (512) 867-8528
HAYNES AND BOONE, LLP	Fax: (214) 200-0853
2801 N. Harwood St., Suite 2300	kelly.lyle@haynesboone.com
Dallas, TX 75201	USPTO Reg. No. 62,332

Hong Shi	Phone: (512) 867-8440
HAYNES AND BOONE, LLP	Fax: (214) 200-0853
2801 N. Harwood St., Suite 2300	hong.shi.ipr@haynesboone.com
Dallas, TX 75201	USPTO Reg. No. 69,009

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

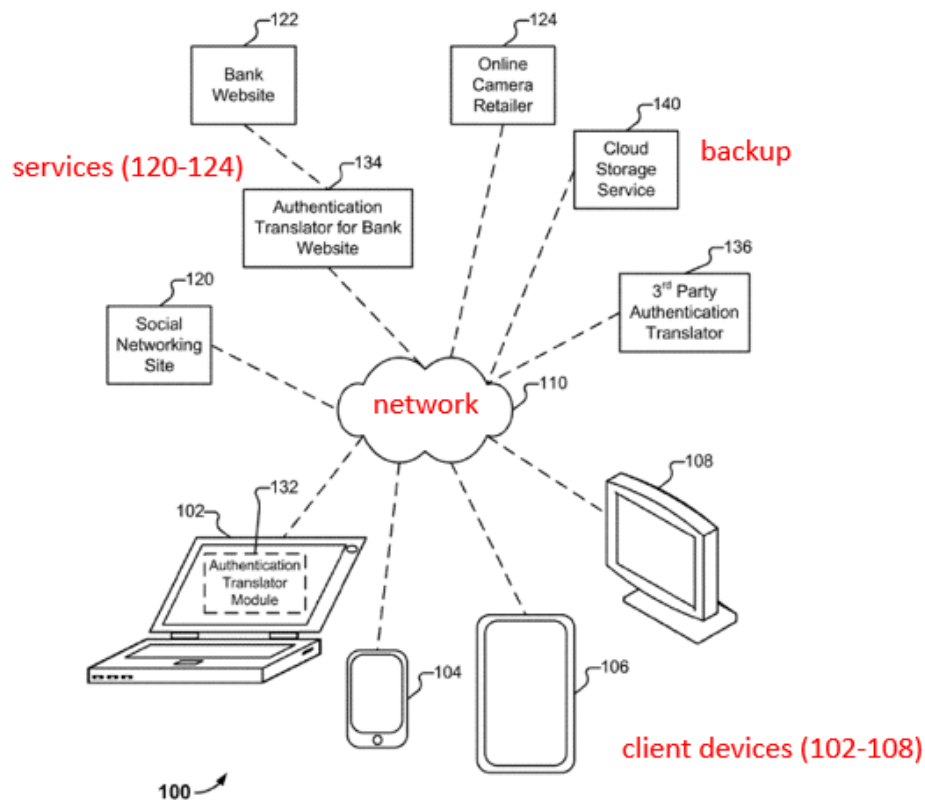
III. GROUNDS FOR STANDING

Petitioner certifies that the '512 patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. §42.104(a).

IV. THE '512 PATENT

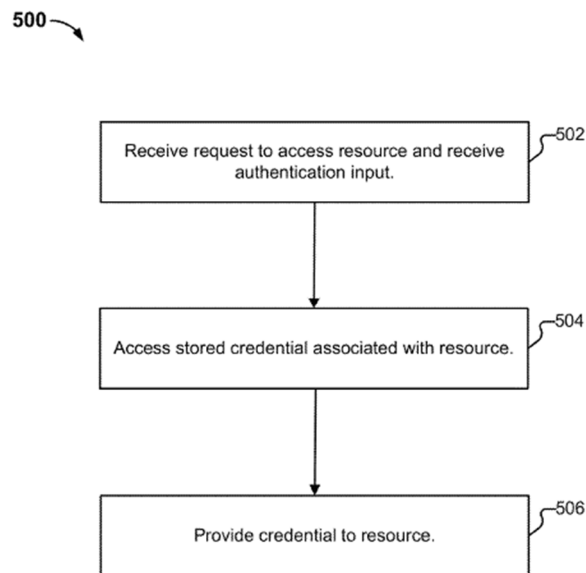
A. Summary of the '512 patent

The '512 patent is directed to an environment including a client device, such as a notebook computer, smartphone, or tablet, which is connected via a network to a service such as a website. APPL-1001, 2:37-56. FIG. 1 is illustrative:



APPL-1001, FIG. 1, annotated

The '512 patent describes authentication techniques to provide user credentials (*e.g.*, a password) from a client device to a service with a goal of avoiding reliance on a user's input of the credential, which is tedious for the user and leads to poor security practices. APPL-1001, 1:35-44. The '512 patent states users "need not type such usernames and passwords into their devices whenever required by a service. Instead, users can authenticate themselves to an 'authentication translator'...and the authentication translator will provide the appropriate credentials to the implicated service on the user's behalf." APPL-1001, 2:63-3:1. FIG. 5 of the '512 patent illustrates a process for performing this authentication translation. APPL-1001, 1:58-59.



APPL-1001, FIG. 5

The '512 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.” *See* APPL-1001, 6:18-31. 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. APPL-1001, 6:39-40. If a match is found, a previously stored credential associated with the resource is provided to the resource. APPL-1001, 6:46-47. *See also*, APPL-1003, ¶¶28-31.

However, as discussed below, these techniques for authentication translation were well-known at the time of the claimed invention. APPL-1003, ¶¶32-51.

B. Prosecution History

There were no office actions or prior art rejections during the prosecution that led to the '512 patent. In a notice of allowance, the Examiner stated that the prior art of record did not teach two limitations of the claims that included facilitating a login and performing a secure backup (*see* limitations [1.6A], [1.6B] directed to “in response to determining...a match...facilitate a login” and limitation [1.7B] directed to “perform a secure backup...”). APPL-1002, 93. These features, just like the other elements of the claims, were well-known to POSITA before earliest priority date of the '512 patent. APPL-1003, ¶31.

V. LEVEL OF ORDINARY SKILL IN THE ART

The level of ordinary skill in the art may be reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Here, Persons of Ordinary Skill in the Art (“POSITA”) at the time of the claimed 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. APPL-1003, ¶¶18-21. Furthermore, a person with less formal education but more experience, or more formal education but less experience, could have also met the relevant standard for POSITA. *Id.* However, Petitioner does not imply that a person having an extraordinary level of skill should be regarded as POSITA.

VI. CLAIM CONSTRUCTION

During IPR, claims are construed according to the standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (*en banc*). 37 C.F.R. §42.100(b) (Nov. 13, 2018). The claims are construed to the extent necessary to resolve the underlying controversy. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioner submits that for purposes of this proceeding, and as set forth below, the terms of the challenged

claims should be given their plain and ordinary meaning. *Phillips*, 415 F.3d at 1314-17; APPL-1003, ¶¶52-56.

A. “restricted interface”

A “*restricted interface*” is an interface that limits accessibility. APPL-1003, ¶53. In the ’512 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). APPL-1001, 4:6-8 (“users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API”). Thus, POSITA would understand *restricted interface* to at least include an API that limits accessibility to a secure storage, a fingerprint sensor, or a dedicated processor. APPL-1003, ¶53.

The Board has addressed this term, *restricted interface*, 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). In IPR2022-00244, the Board referenced (in its description of the ’696 patent) the very same description

noted above (from the '512 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 (APPL-1014)).

In the Parallel District Court Proceeding, Patent Owner proposed (and the court issued a preliminary construction) that the term *restricted interface* is to be understood in accord with plain and ordinary meaning. APPL-1026, 1. Nonetheless, Petitioner is mindful that (in IPR2022-00251 directed to the '512 patent) the term *restricted interface* was central to a non-institution decision that found that petitioner (Samsung) and its expert failed to explain how prior art teachings disclosed a “restricted interface” in part because no express construction was offered. *See* IPR2022-00251, Paper 17, at 23, 25 (PTAB 2002).

Plain and ordinary meaning of “*restricted interface*” is an interface that limits accessibility. Petitioner also demonstrates 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 whether the term is construed as suggested by Petitioner or is merely to be understood in accord with plain and ordinary meaning.

VII. REQUESTED RELIEF

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

VIII. OVERVIEW OF CHALLENGES

A. Challenged Claims

Claims 1-6, 10-16 and 20-21 (“Challenged Claims”) of the ’512 patent are challenged.

B. Statutory Grounds¹ for Challenges

Ground	Claims	Basis
#1	1-6, 10-16 and 20-21	§103(a) over Kesanupalli in view of Challener and Cheng

Kesanupalli was filed March 24, 2010, published April 7, 2011, and issued August 5, 2014. Challener was filed September 29, 2006, published May 1, 2008, and issued January 17, 2012. Cheng was filed September 24, 2003 and published June 17, 2004. Kesanupalli and Challener are prior art under at least pre-AIA §§102(a), (e). Challener’s PG-PUB (APPL-1022) is also prior art under §102(b). Cheng is prior art under §102(b).

¹ Pre-AIA §§102, 103(a) apply.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1-6, 10-16 and 20-21 are Rendered Obvious under §103(a) over Kesanupalli, Challenger and Cheng

1. Kesanupalli

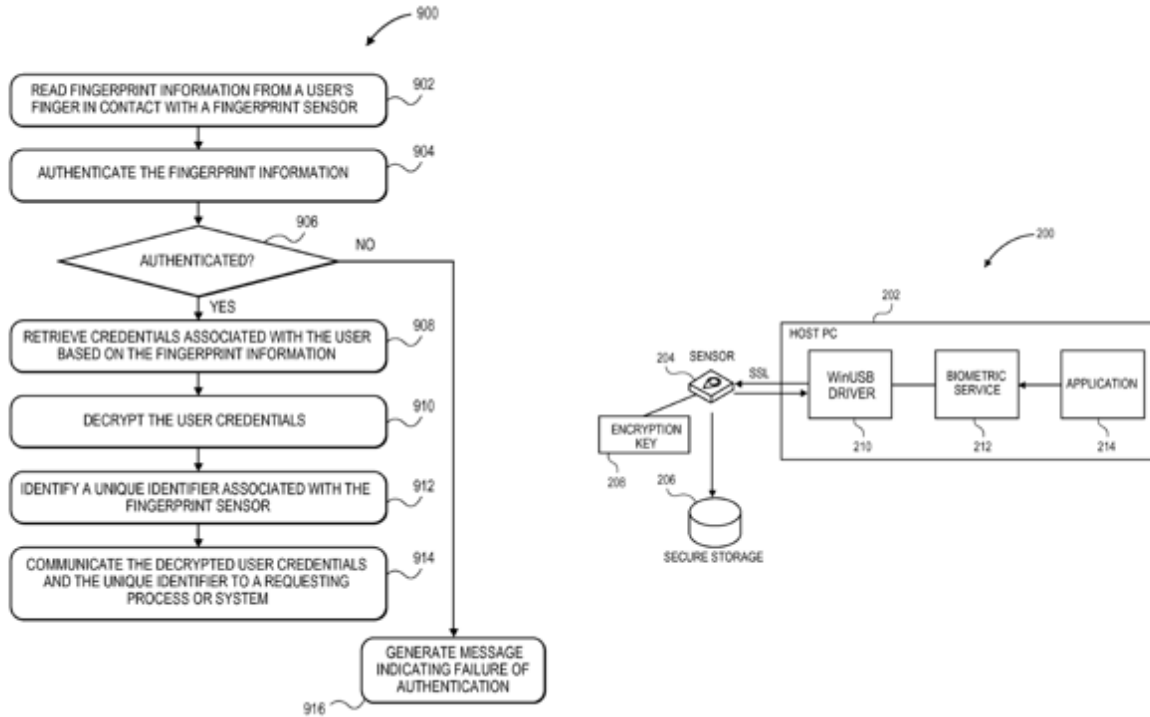
Kesanupalli is entitled “Secure User Authentication Using Biometric Information” and is directed to a secure authentication system that uses biometric information to “provide[] a more secure authentication of the user than commonly used password-based methods and systems.” APPL-1006, (54), 1:59-62. For 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. APPL-1003, ¶¶61-66; APPL-1006, FIGS. 8-9, 3:14-4:11.

During an enrollment process with a resource such as a website, “a user swipes [or places] their finger [on] a fingerprint sensor several times to create [the] fingerprint template. The fingerprint template allows the user’s fingerprint to be distinguished from fingerprints associated with other users.” APPL-1006, 3:33-41. The user (or system) also “provides user credentials, such as a password, cryptographic key...or the like,” and the systems and methods described in Kesanupalli “bind the user’s fingerprint template with the user credentials.” APPL-1006, 3:15-18, 3:41-46. To protect user credentials, “[t]he fingerprint template and

user credentials are then stored in a secure storage of the user's device.” APPL-1006, 3:46-47, *see also*, APPL-1006, 8:29-53.

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

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. APPL-1006, 6:26-49.



APPL-1006, FIGS. 9 and 2

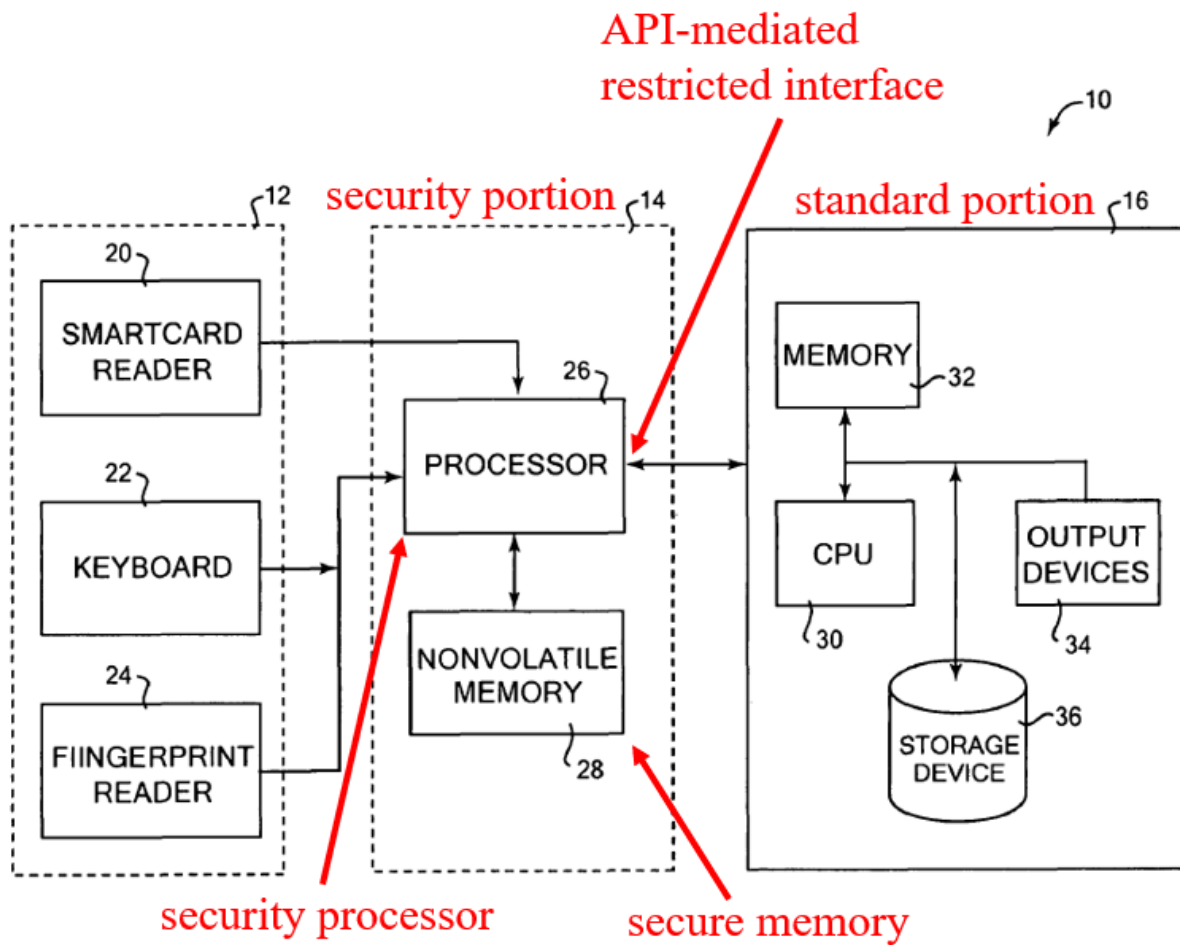
In an authentication process such as discussed above, the biometric sensor 204 receives a biometric input from a user and releases the user's credentials from secure storage 206 upon a successful match of the input with the user's stored biometric template. APPL-1006, 6:31-45. The released credentials are then communicated to the external resource by an application 214 of the Host PC 202. APPL-1006, FIG. 2, 5:9-58, 6:11-31.

2. Challenger

Challenger "relates to securely protecting computer data, and more particularly to security processors provided in computer systems to implement security features." APPL-1007, 1:7-9, 3:24-26. Challenger illustrates a system 10 (e.g., computer or

electronic device) with a system architecture suitable for securing data and functions of system 10 from unauthorized access and manipulation. APPL-1007, 3:37-56. In particular, Challenger 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* APPL-1007, 3:51-56. As explained in Challenger, 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. APPL-1003, ¶¶67-69, 45-51.

Broadly speaking, TPMs provide a platform for effective trusted computing features. APPL-1003, ¶68. The security architecture (*i.e.*, the functions and the application programming interface (API)) that runs on the microcontroller) can be referred to as a TPM. A TPM can offer a variety of functions, including a random number generator, facilities for secure generation of cryptographic keys, and abilities to limit the use of keys, *e.g.*, to signing and verification, and/or encryption and decryption. APPL-1007, 1:18-31.



APPL-1007, FIG. 1, annotated

Challenger 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. APPL-1007, 3:46-57. Security portion 14 is used to secure data and provide applications for access and use only by authorized users through a dedicated security processor 26 and a memory 28. APPL-1007, 4:9-65. The nonvolatile memory 28 is connected to the secure 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 and includes a microprocessor (CPU) 30 that controls general operation of the system including input/output functions. APPL-1007, 5:15-25.

3. Cheng

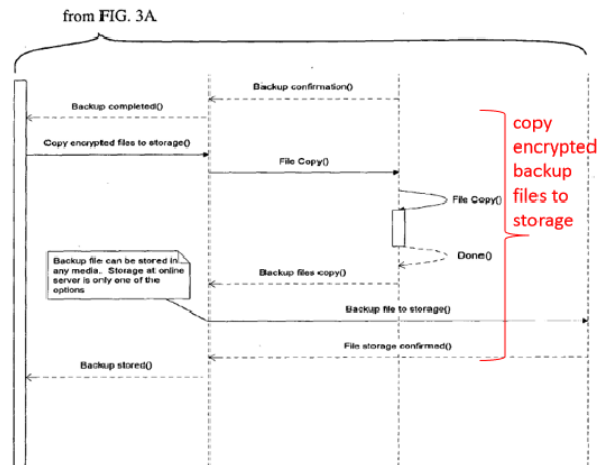
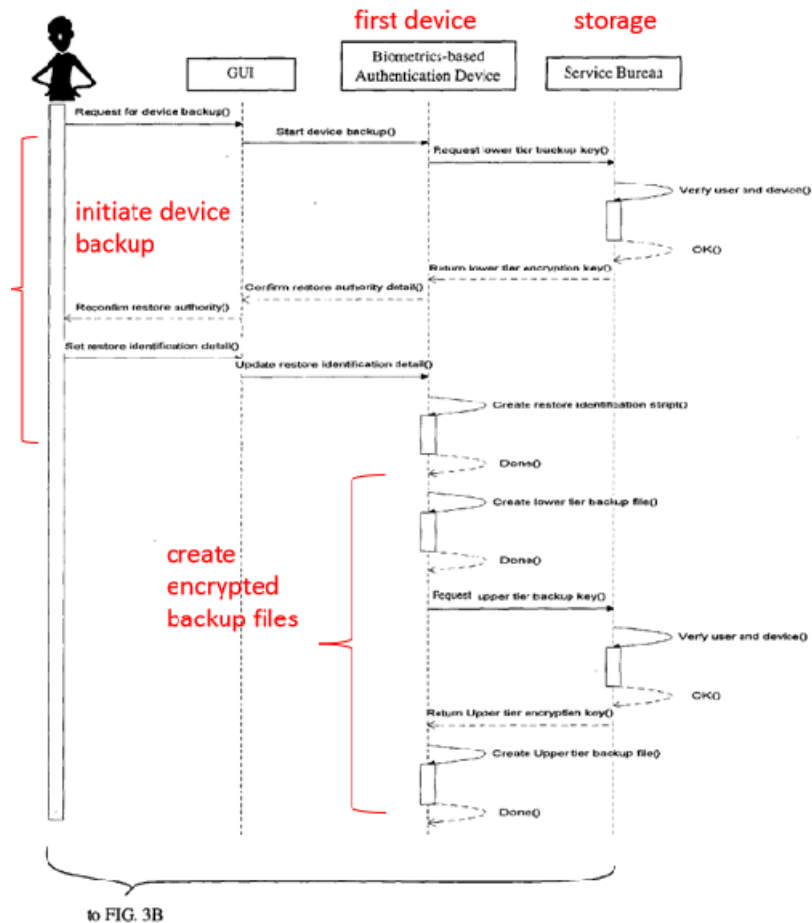
Cheng is entitled “System, Method and Apparatus for Secure Two-Tier Backup and Retrieval of Authentication Information” and provides ways to “securely backup and restore” a user’s authentication-based device without compromising the security thereof. APPL-1008, (54), Abstract.

Cheng recognizes “[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.” 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.* According to Cheng, “[b]iometrics-based authentication” is commonly implemented, which leads to portable devices that include “user’s authentication information, electronic identity and any data associated therewith.” APPL-1008, [0004], [0006].

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

on new device from scratch should a first device containing the data be lost or stolen.

See APPL-1003, ¶¶70-73; APPL-1008, Abstract, [0006]. An exemplary backup process is illustrated in Cheng's FIGS. 3A-3B where backup of data of a first user's device is performed through secure communication between a user service bureau (storage) and the device. APPL-1008, [0029]-[0030]. Cheng's backup process includes a two-tier encryption of the backed-up data. APPL-1003, ¶72; APPL-1008, [0031]-[0039].



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

Cheng describes a use case of a user's first device, having been backed-up to a user service (a storage service), becoming unavailable. A secure connection is provided between the user service and a second device to retrieve the backed-up data downloaded to the second device. *See* APPL-1008, [0044]–[0050], FIGS. 4A-4C.

4. Overview of Kesanupalli and Challenger Combination

As demonstrated by the discussion of Kesanupalli (*see* Section IX.A.1), Kesanupalli discloses the authentication translation techniques espoused by the '512 patent, including obtaining biometric input from a user, comparing the biometric input to authenticate the user, and if matching, transmitting appropriate credentials of the user to the associated service on the user's behalf. Kesanupalli also describes and illustrates example systems (including that of FIG. 2) on which these techniques may be performed. For example, sensor 204 is capable of receiving and authenticating biometric information and communicating with its secure storage 206, which stores the user credentials and biometric templates, and on successful authentication, releases the user credential. APPL-1006, 6:26-49. A computing host (PC) 202 receives information from sensor 204 and communicates with external resources. APPL-1006, 6:26-31; 5:59-6:25 (describing similar components relative to FIG. 1).

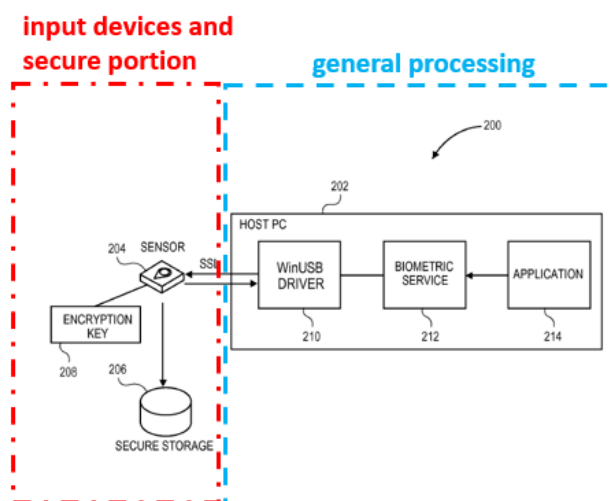
Kesanupalli explains that these components can be manufactured together in a single device, or separately. APPL-1006, 2:48-50. POSITA would have

understood Kesanupalli's techniques are achieved through processor(s) executing the described functions including those of sensor 204 (*e.g.*, matching, decrypting, etc.) and Host PC 202 (*e.g.*, executing applications 110, 112). APPL-1003, ¶¶74-79. APPL-1006, 6:28-49, 5:62-64 (describing similar components relative to FIG. 1). Kesanupalli suggests that specialized or general processors may perform its tasks. APPL-1006, 6:11-17, 6:42-45, 9:58-10:12.

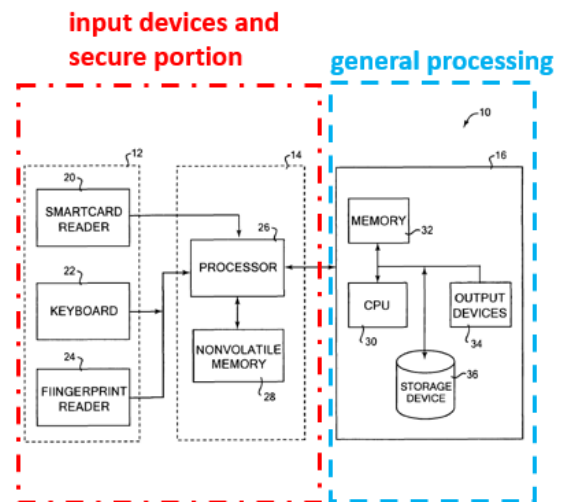
A well-known platform for implementing secure systems and for securely handling sensitive information is a Trusted Platform Module (TPM) security architecture. APPL-1003, ¶¶77, 45-51. TPM implementations were widely implemented based on specifications from Trusted Computing Group (TCG) and would have been well understood by POSITA before the earliest priority date of the '512 patent. *Id.* Challenger, discussed in Section IX.A.2, is a TPM implementation and is generally illustrative of a TPM architecture adapted to a biometric security application. More specifically, Challenger provides a specialized processor—a security processor—that performs security functions, receives input from an authentication device and communicates with a main processor, which performs general tasks including connecting to external resources. APPL-1007, FIG. 1, 3:58-36, 5:15-25, 5:35-40.

Challenger's TPM security architecture would have been an attractive platform on which to implement a biometric security system such as that described in

Kesanupalli, particularly for POSITA who would value a proven, widely adopted security architecture and who would expect that the marketplace would favor a standards-based implementation. APPL-1003, ¶78. Additionally, Challenger's description of TPM architecture would have been an attractive implementation platform because of the correspondence of general and secure processor portions, secure storage, and a fingerprint reader described in Challenger's TPM based implementation with functional blocks described in Kesanupalli. APPL-1003, ¶¶78-79.



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

Referring to annotated figures above, Kesanupalli and Challenger each involve a **first portion**—annotated blue—that executes applications, performs general computing tasks and communicates with external resources and a **secure second portion**—annotated red—that executes functions for accepting biometric input,

performing authentication, and securely storing the associated data. POSITA would have been motivated to implement Kesanupalli's functionality on Challenger's TPM architecture using a specialized security processor (e.g., Challenger's security processor 26 including its APIs) to isolate the secure functions of Kesanupalli's sensor 204 and secure storage 206, while hosting on a general processor (Challenger's microprocessor 30) the applications and other functions of Kesanupalli's Host PC 202. APPL-1003, ¶79. Challenger's TPM-based decomposition into secure and general processor portions would have provided a well-known and standardized security architecture and a natural fit for performing the respective functions described by Kesanupalli. *Id.*

5. Reasons to Combine Kesanupalli and Challenger

Continuing the discussion above, POSITA would have been motivated to apply Challenger's teachings of a TPM-type security architecture to Kesanupalli's techniques to provide a security processor (a second processor as discussed below) in a secure portion communicating with a general processor (a first processor as discussed below) in a standard portion with API-mediated interfaces of the second processor in between. APPL-1003, ¶¶80-84. The combination would have produced the obvious, beneficial, and predictable results of a standardized and widely-deployed security architecture (TPM) for implementation of Kesanupalli's techniques as discussed below. *Id.*

First, Challener, Kesanupalli and the '512 patent are analogous art and are all in the same field of endeavor—namely, information security, and more particularly, security arrangements for protecting computers, components thereof, programs or data against unauthorized activity. APPL-1003, ¶¶81-82; 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”); 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.”); APPL-1001, 1:35-44 (“Providing credentials to a service, whether via a mobile or other device, is often a tedious experience for a user...[U]sers will often engage in practices...which render their credentials less secure against attacks. Accordingly, improvements in authentication techniques would be desirable.”), FIG. 1 (showing client devices of notebook computer 102, smartphone 104, tablet 106).

Moreover, as evidenced on the front pages of Challener, Kesanupalli and the '512 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 (security arrangements for protecting computers, components thereof, programs or data against unauthorized activity). *See* APPL-1001, (51), (52); APPL-1006, (51) (58); APPL-1007, (51).²

Second, POSITA would have been motivated to apply Challenger’s teachings of a standards-based TPM architecture as an implementation framework for Kesanupalli’s biometric security techniques given the support a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided. APPL-1003, ¶83; APPL-1007, 1:18-31 (summarizing typical TPM functions and APIs). Indeed, Challenger’s description of its TPM-based security architecture includes *both* secure storage (nonvolatile memory 28) for secure data, *e.g.*, “secure hash values and...keys,” *and* fingerprint reader 24 behind a security processor 26 that “implements the particular security features and functions (*e.g.*, API functions, algorithms)” in a system that includes secure and non-secure portions. APPL-1007,

² *see also* www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (subclass definitions); www.uspto.gov/web/patents/classification/cpc/html/cpc-G06F.html#G06F (CPC to IPC concordance).

4:57-5:9, 3:67-4:23. These are precisely the security architecture features POSITA having Kesanupalli before them would be motivated to implement in a standards-based security architecture that would engender trust amongst users and customers. APPL-1003, ¶¶83, 48-51; APPL-1016; APPL-1017 (describing TPM adoption).

Finally, POSITA would have had reasonable expectations of success in implementing Kesanupalli's biometric authentication techniques in Challener's TPM-based architecture, as TPMs were well-known, standard and widely-deployed in the industry. APPL-1003, ¶¶84, 51. *See* APPL-1007, 1:18-31, *see* Section IX.A.2. Further, Kesanupalli itself suggests the user of specialized processors. APPL-1003, ¶84; APPL-1006, 9:64-10:1.

6. Reasons to Combine Kesanupalli, Challener and Cheng

In addition to implementing Kesanupalli with Challener's TPM architecture, as discussed above, POSITA would have had been motivated to apply Cheng's teachings of backing-up data of a device, such as the data of Kesanupalli's device including biometric information and credentials for user authentication. APPL-1003, ¶¶85-91. Kesanupalli in view of Challener has stored biometric information and credentials, which are a user's personal data stored in a user's first device, which combined with Cheng's backup teachings applied would produce the obvious, beneficial, and predictable results of reducing the need to recreate the user's personal data on a new device (*e.g.*, a second device replacing a lost or stolen first device).

Id.

Furthering the discussion above with respect to Kesanupalli, Challenger and the '512 patent's shared field of endeavor, Cheng is also in a same field of endeavor—security arrangements and procedures for protecting data in computer systems. *See, e.g.*, Section IX.A.5, APPL-1008, [0003], [0004] (“computers, electronics, communications, networks, and the Internet, access control in general and network security in particular have come increasingly important...[d]ata, 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.”). While Cheng lacks an explicit search classification, POSITA would recognize a similar field of endeavor in Cheng's disclosure. APPL-1003, ¶¶86-87; APPL-1008, [0007] (“Enabling technologies include biometrics, authentication, cryptography, and encryption/decryption.”)

Second, POSITA would have been motivated to employ Cheng's backup technique in connection with Kesanupalli's secure user authentication methods as implemented by Challenger's architecture because Kesanupalli's stored biometric information and credentials are personal data. APPL-1003, ¶88. POSITA would have understood the stored personal data (biometric information and credentials) would need to be created and registered from scratch should the device be lost or

stolen. *Id.*, APPL-1008, [0006]. Such a problem of inconvenience would have also been reasonably pertinent to the inventor of the challenged patent. *See* APPL-1001, 8:18-21 (noting “[s]ince user data can be frequently backed up [] and recovered [], inconvenience to the user will be minimized” [when wiping a device]”). Thus, not only were Kesanupalli as informed by Challener/Cheng and the ’512 patent in the same field of endeavor, but Cheng would have been reasonably pertinent to a problem faced by the inventor of the ’512 patent and pertinent to known risks of theft and loss of devices and recovery of data that POSITA would have been motivated to address by combining Cheng with Kesanupalli/Challener. Further, POSITA would have recognized a desire in the market for electronic devices to be capable of being backed-up long before the ’512 patent. APPL-1003, ¶90, APPL-1020. Cheng provides a benefit of the desired backup of personal data to provide access to it in other user devices in a “reliable and secure way[]”. *Id.* And Cheng specifically teaches backing-up personal data related to biometric information and secret keys. APPL-1008, [0007] – [0009]. This is data just like the data stored in Kesanupalli’s device. APPL-1006, 3:32-51.

Finally, POSITA would have had reasonable expectations of success in adding backup feature such as taught by Cheng in a biometric authentication system such as taught by Kesanupalli in view of Challener as all are similarly directed to handling of personal information including biometric authentication information in

a secure manner. APPL-1003, ¶91. Adding a backup feature would merely have been applying a known technique to a known device (method, or product) ready for improvement to yield predictable results. Indeed, the backup feature is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli and Challenger’s systems and devices. *Id.*

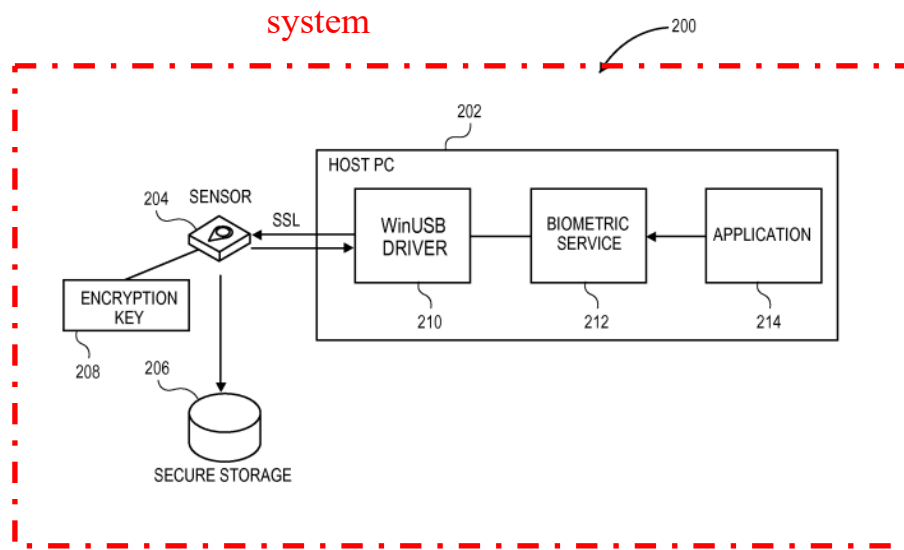
7. Claim 1

[1.0] *A system, comprising:*³

To the extent the preamble is limiting, Kesanupalli (in combination with Challenger) renders obvious *a system* of claim 1. APPL-1003, ¶¶92-95.

As illustrated above, Kesanupalli describes in its FIG. 2 a system 200 “capable of performing biometric user enrollment and authentication.” APPL-1006, 2:1-2; *see also*, APPL-1006, Abstract, FIGS. 11-12.

³ All emphasis in quoted material has been added. Claim terms are *italicized*.



APPL-1006, FIG. 2, annotated

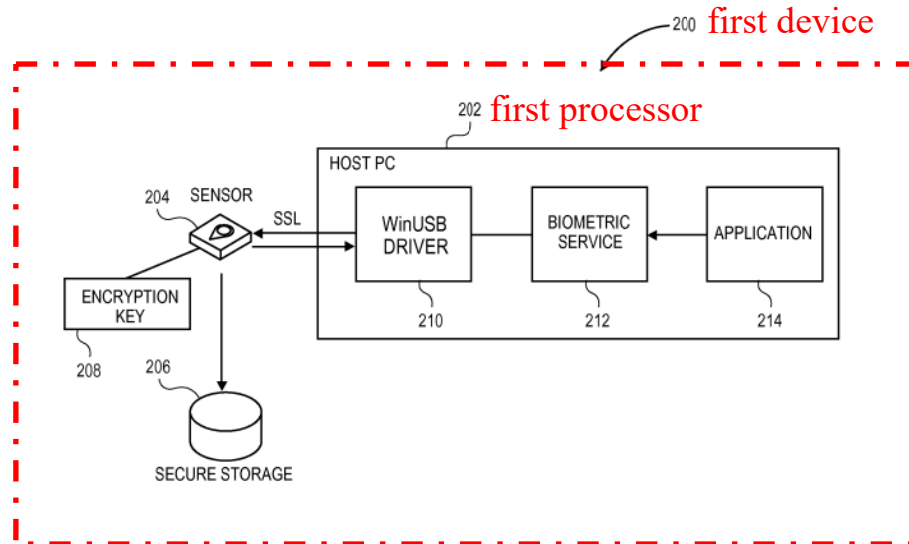
In Kesanupalli's system 200, the sensor 204, including its secure storage 206, provides authentication translation and communicates with Host PC 202, which provides communication with external web servers including the communication of the user credential to a website. *See* APPL-1006, 6:11-49, FIG. 12, 2:54-3:13, 5:44-48. Challenger describes a known architecture that POSITA would have applied to Kesanupalli, including as discussed above, to form the *system*. APPL-1003, ¶¶74-84; *see* Section IX.A.4; *see also*, APPL-1007, FIG. 1, 3:45-4:65.

Thus, Kesanupalli and Challenger (in combination) render obvious *a system*, as claimed as detailed below.

[1.1A] *a first processor of a first device, wherein the first processor is configured to:*

Kesanupalli and Challener render obvious this limitation. APPL-1003, ¶¶96-101.

Individually and in combination, Kesanupalli and Challener disclose *a first device* including *a first processor*. Turning first to Kesanupalli, annotated FIG. 2 illustrates *a first device* including *a first processor*.



APPL-1006, FIG. 2, annotated

Biometric sensor 204, its secure storage 206, and Host PC 202 (including web browser application executing thereon) constitute *a device* that provides authentication translation and ultimately communicates user credentials to web servers. APPL-1003, ¶¶99; APPL-1006, Abstract, 2:54-3:3, 4:3-11, 4:36-50, 6:11-49.

POSITA would appreciate Kesanupalli's embodiments (*e.g.*, FIG. 2) constitute a *device*, generically defined in claim 1 and the '512 patent. APPL-1003, ¶99; APPL-1001, 2:18-20. To the extent that Patent Owner imparts some more integrally-formed meaning to the term, POSITA would also understand Kesanupalli to disclose integrally-formed realizations of *a first device*. APPL-1003, ¶99; APPL-1006, 2:48-50 ("In particular embodiments, the biometric sensor is **physically attached (or manufactured into) a client device** such as a computer, cellular phone, and so forth. which also includes the sensor 204"), 3:47-51 ("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.")

As discussed in Section IX.A.4, POSITA would have implemented Kesanupalli's system 200 and techniques performed by the system using the TPM-based architecture of Challenger. In doing so, the functions of HOST PC 202 (which are performed by a processor) including communication with an external resource as discussed below, are implemented as *first processor*, which is a general processor shown in Challenger as general microprocessor 30. APPL-1003, ¶¶100, 74-79; APPL-1006, 2:54-3:3, 6:11-25, 9:58-10:12 (discussing PC 202 functions executing on a processor); APPL-1007, FIG. 1, 5:15-25 (discussing similar functions of general microprocessor 30).

Thus, Kesanupalli and Challenger (in combination) render obvious “*a first processor of a first device*” configured to perform the functions now detailed with respect to successive limitations.

[1.1B] [*wherein the first processor is configured to*] *based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource;*

Kesanupalli and Challenger render obvious this limitation. APPL-1003, ¶¶102-111.

Kesanupalli discloses that *based at least in part on a request associated with a user to access an external resource* (e.g., user visiting a website), the first processor performs the action of *establish[ing] a secure connection with the external resource* (website). As discussed above, Kesanupalli discloses an enrollment process, where the user visits an *external resource* (website) to enroll with the resource and create, and store, the user’s fingerprint template and user credentials associated with the website. *See* Section IX.A.1, *see also*, APPL-1006, 5:33-43, FIGS. 7 and 11 (directed to the enrollment process).

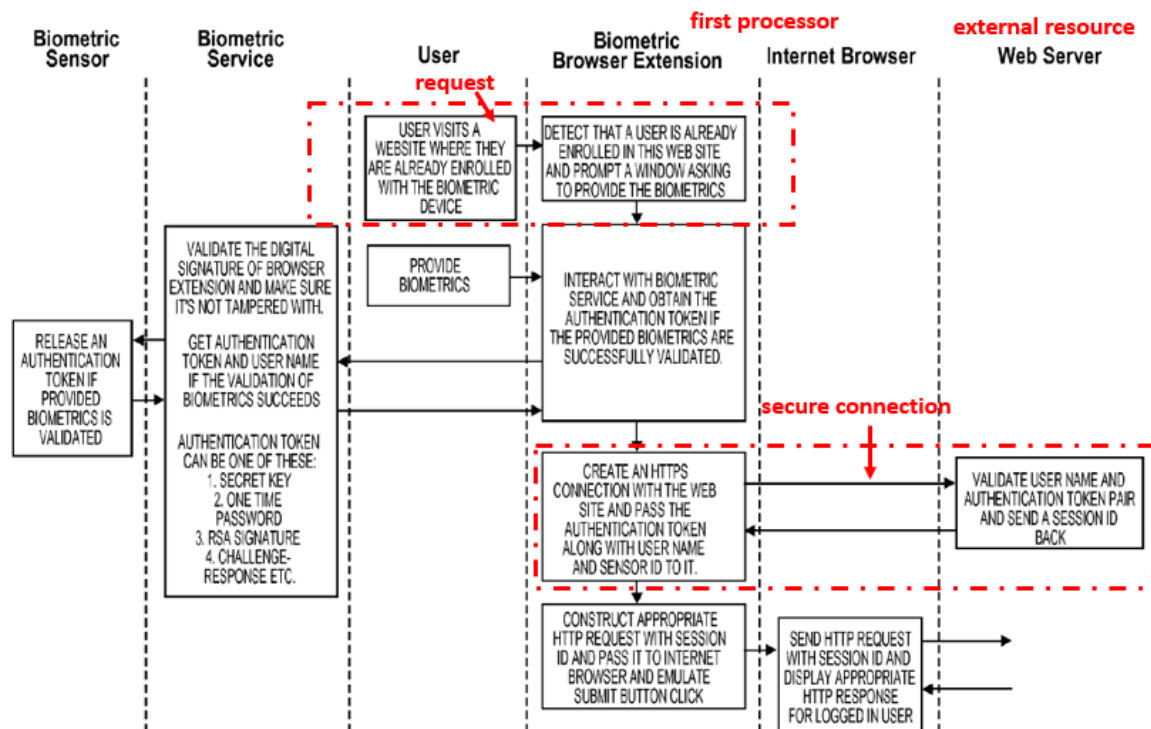
After enrollment, subsequent visits by the user to the external resource initiate an authentication translation procedure. In particular, Kesanupalli describes *a request* (user’s request in accessing website to which she has enrolled) *to access an external resource* (website). APPL-1006, 4:36-5:14 (“...When a **user accesses the Web site**, the Web browser plug-in is activated and detects that a biometric sensor

is installed in the user's computing device. The Web site suggests that the user enroll with their biometric sensor to provide a more secure user authentication...After a user has enrolled with a particular Web site that supports biometric authentication, **subsequent visits to the same Web site** cause the Web browser plug-in to detect that the user has already enrolled with the Web site. In this situation, the Web site prompts the user to perform user authentication (e.g., using the biometric device).”) *See also*, APPL-1006, 2:54-3:3, FIGS. 10, 11.

Based at least in part on this user request to access the website with which she has previously enrolled, Kesanupalli *establishes a secure connection with the external resource* (website). Referring to the system of FIG. 2, this connection is provided between application 214 of PC 202 and the external resource, website on the web server. APPL-1006, 2:54-3:3 (an application is “capable of communicating with one or more web servers or similar devices via the Internet or other data communication network”), 4:36-50, 6:11-50, 7:67-8:4, 9:58–10:1. As discussed above, application 214 is executing on the *first processor* of PC 202, and, as such, the first processor establishes a connection, via the Internet, with a web server of the website. APPL-1003, ¶¶101-105; APPL-1006, 6:11-31, FIG. 9, block 914. Challenger confirms that a *first processor*, microprocessor 30 of a standard portion of a system, performs typical device functions including input/output (communications), which would include Kesanupalli’s connections to external

resources. APPL-1007, 5:15-25. Kesanupalli describes the connection between PC 202 and the web server as a “**secure communication link**,” which is a *secure connection*. APPL-1003, ¶¶104, 110; APPL-1006, 7:54-8:5, 12:62-67.

Kesanupalli’s FIG. 12 illustrates actions for authenticating a user, including those performed by a “user” and those performed by the *first processor* (e.g., PC 202 providing biometric service, browser extension, browser applications) or the external resource’s web server. FIG. 12 also shows communication over the *secure connection* between the first processor and the webserver providing the *external resource*. APPL-1003, ¶108.



APPL-1006, FIG. 12, annotated

Thus, Kesanupalli and Challenger disclose this element as *first processor* (Kesanupalli PC 202/Challenger microprocessor (CPU) 30) *based at least in part on a request associated with a user to access an external resource* (user's visit to a website with which she is/has enrolled), *establish a secure connection with the external resource* (secure communication link illustrated between PC 202 (application 214) and the webserver). Kesanupalli and Challenger (in combination) render obvious “[*the first processor is configured to*] *based at least in part on a request associated with a user to access an external resource, establish a secure connection with the external resource.*”

[1.1C] *and [the first processor is configured to] communicate with a second processor using a restricted interface,*

Kesanupalli and Challenger render obvious this limitation. APPL-1003, ¶¶112-120.

In Kesanupalli's system 200, Host PC 202 communicates with sensor 204. APPL-1006, FIG. 2, 6:17-20. In the Kesanupalli-Challenger combination introduced above (*see* Section IX.A.4), POSITA implementing the security functions of Kesanupalli's sensor 204 would have been motivated to build on the functions of Challenger's TPM-based security architecture using a specialized security processor—a *second processor*—such as illustrated by Challenger's security processor 26. APPL-1003, ¶¶74-79 (explaining the mapping of secure portion functions of Kesanupalli's system to a corresponding secure portion of the TPM

framework implemented by Challener); APPL-1007, 4:9-24, FIG. 1. The *first processor* (Kesanupalli's HOST PC 202 functionality operating in standard portion 16 of Challener's TPM framework) *is configured to communicate with* this security processor, *a second processor*. APPL-1003, ¶¶113-114; *see* APPL-1006, 6:39-42 ("The biometric sensor 204 creates a secure communication with Host PC 202 using SSL v3 protocol or other secure communication technique."). Challener also illustrates—and Kesanupalli's functionality implemented using Challener's TPM-based framework maintains—communication between a first processor (general processor of microprocessor 30) and second processor (security processor 26). APPL-1003, ¶114; APPL-1007, FIG. 1, 5:15-25 ("the standard portion 16 of system 10 is connected to the processor 26").

This communication between the first processor and the second processor uses a *restricted interface*. As explained above, "*restricted interface*" is an interface that limits accessibility. *See* Section VI.A. Furthermore, based on the '512 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.A; APPL-1003, ¶¶114-119. Thus, when Kesanupalli is implemented using Challener's TPM framework for secure systems communication between the security processor executing the functions of sensor 204 (and secure storage 206) and the standard portion of the device (the general processor

executing the functions of PC 202) occurs through a *restricted interface* as detailed below. *Id.*

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 to restrict access to the TPM (secure processor, here *second processor*) by programs running on a general processor (here *first processor*) in a standard (non-secure) portion of a system. APPL-1003, ¶116. In particular, the access is limited to protect the security-related operations and data, such as key and credential management, secure storage, encryption, decryption, and digital signatures, that are provided or maintained in a secure portion of the system. *Id.* See also, APPL-1007, 4:3-15 discussing controlling “access.” The Board has itself recognized, in the context of the related ’696 patent, that TPM implementations disclose a “*restricted interface*.” See (Samsung ’696 Patent IPR) IPR2022-00244, Paper 17, 40.

Challenger discloses an interface (an API) used in its TPM-based architecture in the communication between the *first processor* and the *second processor*. More specifically, Challenger’s secure processor 26—the *second processor*—implements a security architecture that includes API functions used in its communication with other components, including general microprocessor 30—the *first processor*. APPL-1003, ¶¶117-118; APPL-1007, 4:9-24 (“The **processor 26 typically**

implements a ‘security architecture’ which, as used herein, refers to the particular security features and functions (e.g. **API functions**, algorithms) implemented for the system 10 as determined by a security architecture application loaded on the processor 26.”), FIG. 1. As a general proposition, an API is an interface that defines how two or more components—here software executing on secure processor 26 and software executing on general microprocessor 30—communicate with one another. APPL-1003, ¶119. And a TPM-based API, such as provided by Challenger’s secure processor 26, provides restrictions by the way of a set of rules or restrictions POSITA would understand are defined by the TPM standard for access to the security portion of the system. APPL-1003, ¶¶117-119, 51.

Thus, implementing Kesanupalli using the architecture of Challenger provides communication between a *first processor*—general processor (microprocessor 30 executing the functions of PC 202) of a general portion of the TPM-based system—and a *second processor*—a security processor (secure processor 26 executing functions of sensor 204) of a security portion of the TPM-based system, where this communication is via a *restricted interface* (e.g., via an API of the TPM security architecture of the security processor executing the processor functions of sensor 204). This is merely a predictable use of a known element according to its established function in the TPM architecture. APPL-1003, ¶118.

Moreover, POSITA would have understood the API-type interface between

processors in Kesanupalli implemented on Challenger's architecture limits access to security functions and data on the secure processor—in short, it provides, using TPM standardized techniques, a *restricted interface*. APPL-1003, ¶119. Such restrictions limit access and thereby protect the functions and data in the security portion of a TPM-based security architecture (e.g., sensor 204 and the secure storage 206) from being misused by an untrusted or malicious program. *Id.*

Thus, Kesanupalli and Challenger (in combination) render obvious limitation [1.1C], “[*the first processor is configured to*] *communicate with a second processor using a restricted interface,*” and limitation [1.1] in its entirety.

[1.2] *wherein the second processor is configured to:*
 receive a biometric input from a sensor, 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

Kesanupalli and Challenger render obvious this limitation. APPL-1003, ¶¶121-124.

As described above with reference to limitations [1.1A], [1.1C] and Sections IX.A.4, IX.A.5, POSITA would implement Kesanupalli using the TPM-based architecture and provide a security processor—a *second processor on the device*—executing the functions of Kesanupalli's sensor 204, which include those of limitation [1.2].

First, Kesanupalli describes a *biometric input from a sensor* that is received

by the *second processor* (sensor 204). In one example, Kesanupalli describes that sensor 204 receives a biometric input of a “fingerprint” from a “fingerprint sensor.” APPL-1006, 9:10-24 (“procedure 900 reads **fingerprint information** from a user's finger in contact with a fingerprint sensor (902).”); FIG. 9, 6:31-36, (“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.”); *see also*, APPL-1006, FIG. 8, 8:54-9:3. Kesanupalli not only describes that *biometric input corresponds to a fingerprint*, but suggests other biometric information including those further recited in the recited group. APPL-1006, 2:31-35 (“‘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.”)

Thus, Kesanupalli and Challenger (in combination) render obvious this limitation.

[1.3] *[wherein the second processor is configured to] access a record stored in a secure storage, wherein the record is associated at least with the external resource;*

Kesanupalli and Challenger render obvious this limitation. APPL-1003, ¶¶125-134.

As described above with reference to limitations [1.1A], [1.1C] and Sections IX.A.4, IX.A.5, POSITA would understand that Kesanupalli implemented using the TPM-based architecture of Challenger has a security processor—*a second processor on the device*—executing the functions of Kesanupalli’s sensor 204, which include the limitation [1.3].

Kesanupalli describes a user’s enrollment process for an external resource such as a website where the user’s credential and biometric template are stored in a secure storage. APPL-1006, 3:32-51 (“Initially, a user enrolls with the biometric user authentication system by **binding their user credentials with the user’s biometric template (a ‘fingerprint template’ in specific implementations)**...During an example enrollment process that uses a fingerprint sensor as the biometric sensor, a user swipes their finger across the fingerprint sensor several times to create a fingerprint template...After creating a fingerprint template, the user (or a web server or other system) provides **user credentials**, such as a password, cryptographic key, random seed, and the like. The systems and procedures described herein **bind the user’s fingerprint template with the user credentials**.”)

The fingerprint template and user credentials are then stored in a **secure storage device**.”) Kesanupalli in FIG. 7 walks through this enrollment process. APPL-1006, 8:29-53 (including block 710 where “the procedure binds the user credentials with the fingerprint template[], then stores the user credentials and the fingerprint template [] in a secure storage.”) With respect to FIG. 2, Kesanupalli states “**User credentials** and other information may be **stored** within biometric sensor 204, in a **secure storage 206**, or any other storage mechanism.” APPL-1006, 6:45-47.

The stored user’s credential bound with a biometric template is a *record*, which is *stored on the first device* in a secure storage. APPL-1003, ¶129, APPL-1019, (definition of “record”). The record is *associated at least with the external resource* as the credential and/or the template are associated with the website. APPL-1006, 5:33-5:41 (including “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**.”), 8:47-53 (“In a specific embodiment, the procedure also binds a **particular web site** (*e.g.*, a web site requesting biometric enrollment and/or biometric authentication of a user) **with the**

fingerprint template. Thus, a particular user may perform the biometric enrollment procedure for each web site that the user is to provide future biometric authorization or biometric authentication.”)

Kesanupalli’s secure storage 206 provides the recited *secure storage*. See APPL-1006, FIG. 2, 6:45-47. A *secure storage* is storage protected from unauthorized access. APPL-1003, ¶131. By describing its storage as “secure storage,” POSITA would understand Kesanupalli to be providing a storage protected from unauthorized access. *Id.* As illustrated by Kesanupalli’s FIG. 2, access to secure storage 206 is controlled by sensor 204 and the storage is not directly accessible by others (*e.g.*, application 214 executing on Host PC 202); for example, the user credential in secure storage 206 cannot be accessed (and released) except by sensor 204 (*e.g.*, when verifying a match of biometric input). Challenger likewise maintains storage in a secure portion of a TPM-based architecture is accessible by only its secure processor and thus is a *secure storage*. APPL-1007, FIG. 1, nonvolatile memory 28, 4:57-65 (“A nonvolatile memory 28 is included in security portion 14 and is connected to the processor 26. For example, memory 28 can be Flash memory, Electrically Erasable Programmable Read Only Memory (EEPROM), or other type of memory. In the described embodiment, **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, or package, of the processor 26.”)

Thus, Kesanupalli and Challener (in combination) render obvious “[*wherein the second processor is configured to*] *access a record stored in a secure storage, wherein the record is associated at least with the external resource.*”

[1.4] [i>wherein the second processor is configured to] *retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;*

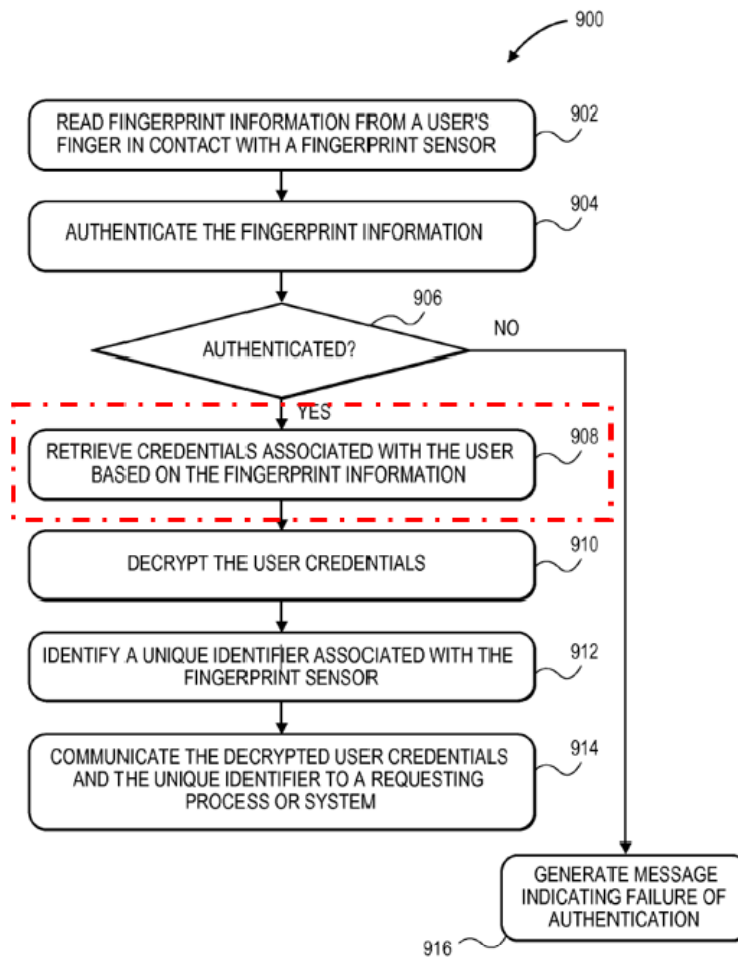
Kesanupalli and Challener render obvious this limitation. APPL-1003, ¶¶135-139.

As described above with reference to limitations [1.1A], [1.1C] and Sections IX.A.4, IX.A.5, POSITA would understand that Kesanupalli implemented using TPM-based architecture has a security processor—a *second processor on the device*—executing the functions of Kesanupalli’s sensor 204, which includes executing the functions of limitation [1.4].

As discussed above for limitation [1.3], in an enrollment process the *record* (template and credential) is stored in secure storage 206 of the first device. And Kesanupalli also describes one type of user credential is a *cryptographic key* and another is a *password*. APPL-1006, 3:41-44 (“user credentials, such as a **password**, **cryptographic key**, random seed, and the like.”) *See also*, APPL-1006, 3:65-4:1, FIG. 12 (referring to “authentication tokens”), 8:6-22.

After enrollment including 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 prompts the user to perform user authentication.”) If successfully authenticated, the *second processor*, security processor executing functions of sensor 204, *retriev[es] from the record* the user credential (*e.g.*, password or key) to release the credential to the requesting resource (website via PC 202). APPL-1003, ¶138. FIG. 9 is illustrative of steps after successful matching includes “the procedure **retrieves credentials** associated with the user.” APPL-1006, 9:17-20.



APPL-1006, FIG. 9, annotated

See also APPL-1006, 3:52-59 (“During an example user identification process (also referred to as a user verification process), a user swipes their finger across a fingerprint sensor. The process then determines whether the user's fingerprint information matches a fingerprint template associated with the fingerprint sensor. If the user's fingerprint information matches a fingerprint template, the user's **credentials are released** to the user and/or a service or process requesting the user

verification.”), 3:65-4:1 (“[T]he **user credentials released** after finding a matching fingerprint template may include an OTP (One Time Password) token, RSA signature and the like”), 6:42-45 (“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.”), FIG. 12 including “Release an authentication token [user credential] if provided biometrics is validated.”

Thus, Kesanupalli and Challener (in combination) render obvious “[*wherein the second processor is configured to*] retrieve, from the record, at least one of a password, a cookie, or a cryptographic key.”

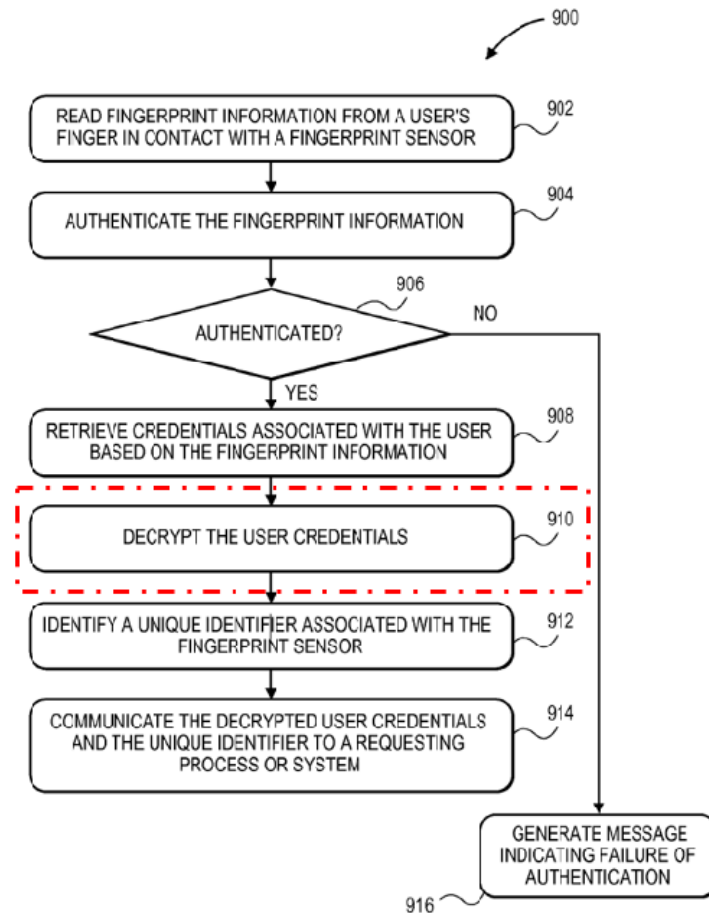
[1.5] [*wherein the second processor is configured to*] perform a cryptographic operation;

Kesanupalli and Challener render obvious this limitation. APPL-1003, ¶¶140-144.

As described above with reference to limitations [1.1A], [1.1C] and Sections IX.A.4, IX.A.5, POSITA would provide Kesanupalli implemented using the TPM-based architecture having a security processor—a *second processor on the device*—executing the functions of Kesanupalli’s sensor 204, which include limitation [1.5].

Kesanupalli as discussed in limitation [1.4] above describes on a successful authentication of a user’s biometric input, retrieving the user’s credentials from the record in storage, on which a *cryptographic operation* is performed by the second

processor (sensor 204). FIG. 9 of Kesanupalli's procedure continues to explain "the procedure retrieves credentials associated with the user based on the fingerprint information (block 908). The **procedure then decrypts the user credentials** (block 910)." APPL-1006, 9:17-21.



APPL-1006, FIG. 9, annotated

See also, APPL-1006, 6:31-49 ("In the example of FIG. 2, the **biometric sensor decrypts the user credentials** only after a successful biometric reading..."), 4:12-

22 (illustrating the example cryptographic algorithms). A decryption is a cryptographic operation. APPL-1003, ¶¶142, 42-44.

As discussed, POSITA would have implemented the sensor 204 functions using a *second processor* according to the TPM-based architecture of Challenger. APPL-1003, ¶143. Challenger also confirms a security processor *is configured to perform a cryptographic operation*. APPL-1007, 4:24-36 (“For example, processor 26 can implement a TPM security architecture, which is a well-known standard for securing computer data...The typical security functions of a TPM include random number generation, secure generation of cryptographic keys, secure storage, abilities to limit the use of keys (such as for signing and verification), and/or **encryption and decryption.**”)

Thus, Kesanupalli and Challenger (in combination) render obvious “[*wherein the second processor is configured to*] perform a cryptographic operation.”

[1.6] [*wherein the second processor is configured to*]

[1.6A] *in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor,*

[1.6B] *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 at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and*

Kesanupalli and Challenger render obvious limitations [1.6], [1.6A] and [1.6B]. APPL-1003, ¶¶145-156.

As described above with reference to limitations [1.1A], [1.1C] and Section IX.A.4, POSITA would implement Kesanupalli using the TPM-based architecture of Challenger providing a security processor—*a second processor on the device*—executing the functions of Kesanupalli’s sensor 204, which include the limitations [1.6A], [1.6B]. As discussed below, this is because sensor 204—the functionality of which is executed on the *second processor* in the applied Kesanupalli-Challenger combination—performs the matching to authenticate the user and in response to a match, transmits output in the form of credentials from its secure storage to the external resource (via the established connection between the first processor and the resource).

As to limitation [1.6A], Kesanupalli’s authentication procedure includes determining that there is *a match between the biometric input (e.g., fingerprint information) and a stored biometric template (e.g., fingerprint template)*. APPL-1006, 9:12-18 (“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).”), 6:34-47 (“For example, in a successful fingerprint swipe, **the swiped fingerprint information matches a fingerprint template** associated with the fingerprint sensor...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.”), 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.”); *see also*, APPL-1006, 5:17-32, 8:54-9:25, FIG. 9 (including “authenticated?”), FIG. 12 (including “biometrics is validated”). Validating or authenticating means matching the template and the biometric input. APPL-1003, ¶143. To the extent it is required by the claim, *a second processor on the device*—the security processor executing the functions of Kesanupalli’s sensor 204—performs this matching.

In response to determining this match, Kesanupalli teaches that sensor 204 retrieves the credentials, which are then transmitted to the requesting external resource, via the established connection with the external resource (via PC 202). APPL-1006, 9:17-24 (“If the fingerprint information is authenticated, the procedure **retrieves credentials** associated with the user based on the fingerprint information (block 908)...The decrypted credentials...are **communicated to a requesting process or system** (block 914).”) *See also*, APPL-1006, FIG. 12, 9:4-9. In the device of FIG. 2, in response to “on-chip matching” performed by sensor 204, the user credential is retrieved from secure storage 206 of sensor 204 and provided to

application 214 of PC 202 for communication to the external resource (e.g., website). APPL-1006, 6:11-49.

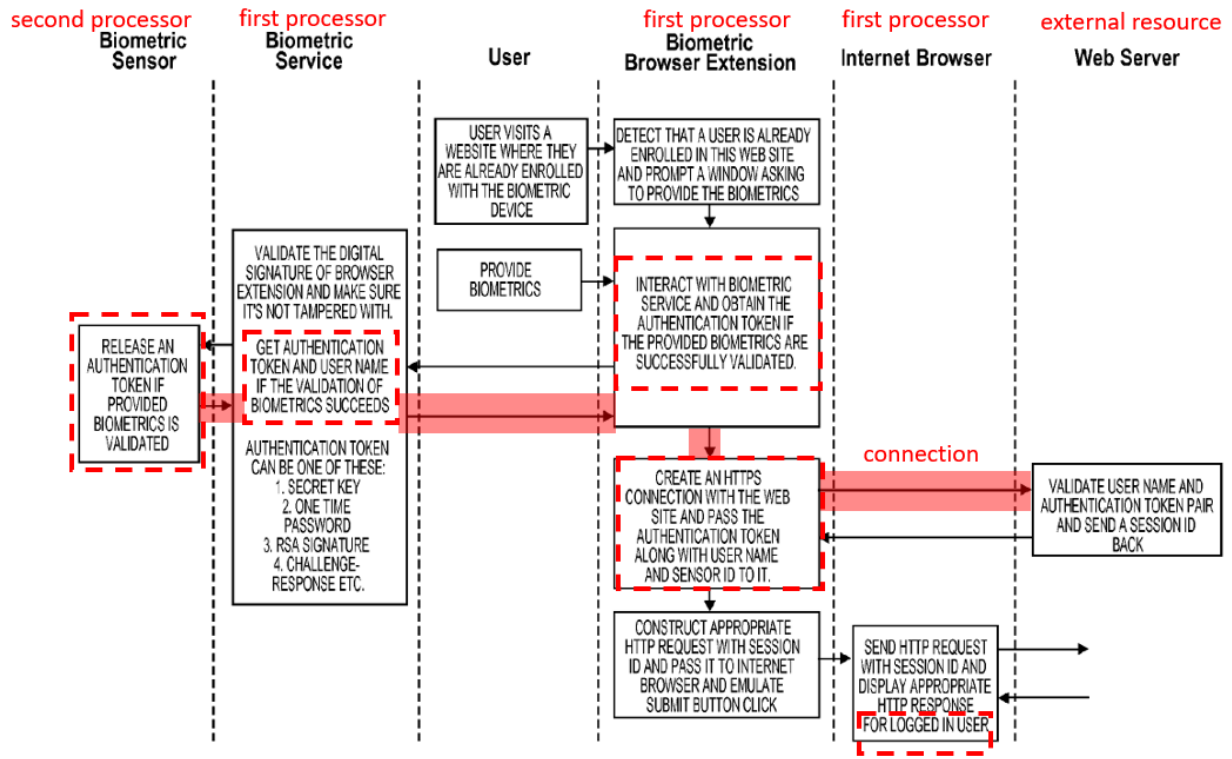
In particular, as to limitation [1.6B], in Kesanupalli's procedure, the security processor executing the functions of sensor 204 (the *second processor*) *facilitate[s] a login of the user to the external resource*. The *second processor facilitates* the login as, in response to verifying the match as in limitation [1.6A], sensor 204 retrieves the credentials from secure storage (206) and transmits, via the HOST PC 202, the credentials (e.g., password, cryptographic key) to the external resource—transmitting the credential to the website, thereby *transmitting output* to the external resource (website). APPL-1006, 9:10-24 (“If the fingerprint information is authenticated, the procedure **retrieves credentials** associated with the user based on the fingerprint information (block 908)...The decrypted credentials...are **communicated to a requesting process or system** (block 914).”) *See also*, APPL-1006, 9:4-9. In particular, in the device of FIG. 2, sensor 204 retrieves the user credential (e.g., cryptographic key) from the secure storage 206 and provides it to PC 202 for communication to the external resource. APPL-1006, 6:11-49. As discussed for limitation [1.1B], a connection is established between the device (in particular application 214 of the first processor of PC 202) and the external resource. Sensor 204 (second processor) sends the decrypted credentials to the website by sending the credentials to application 212 of the PC 202 (*first processor*), and the

PC 202, though application 214, communicates it to the website via this *established connection* between the first processor and the external resource. *See* APPL-1006, 4:1-5, 4:51-63, 5:59-25 discussing application 112, which is substantially the same as application 214 of FIG. 2.

Both Kesanupalli and the '512 patent describe their communication of credentials to website in terms of SSL (now TLS) or HTTPS protocols. *See* APPL-1003, ¶151; *Compare* APPL-1001, 5:7-15 (“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.”), 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. APPL-1023, 2 (summarizing TLS connection initiation and HTTP requests over the initiated TLS connection). Thus, Kesanupalli and the '512 patent describe communication of a decrypted credential to the website via an *established connection* in like manner.

Kesanupalli’s FIG. 12 illustrates actions for authenticating a user, including those performed by a “user,” by the circuitry of the sensor (*second processor*), and by applications on the Host PC (*e.g.*, biometric service, browser extension, browser

applications executed by *first processor*), and by an external resource's web server; it is annotated below illustrating the transmitting of output (user credentials) by the second processor (sensor) to the external resource.



APPL-1006, FIG. 12, annotated

Kesanupalli's transmitting a 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).

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. POSITA would understand when Kesanupalli communicates the credentials “to the Web site to **complete** the user authentication process,” the user login has occurred. APPL-1003, ¶¶154-155; APPL-1006, 5:22-24, FIG. 12 (“logged in user”). This is the purpose of Kesanupalli’s authentication. APPL-1003, ¶¶154-155.

Thus, Kesanupalli and Challenger (in combination) render obvious this limitation, including each portion as delineated above.

- [1.7] *[wherein the second processor is configured to]*
- [1.7A] *perform a secure backup of the record to a storage service,*
- [1.7B] *wherein a second device associated with the user is registered with the storage service, and*
- [1.7C] *wherein the record is downloaded from the storage service by the second device; and*

Kesanupalli, Challenger and Cheng render obvious limitation [1.7], including its sub-portions [1.7A], [1.7B] and [1.7C]. APPL-1003, ¶¶157-175.

Cheng describes a backup technique that provides data of a first device to a storage service such that it is accessible for download by a second device as discussed below, and it would have been obvious to implement Cheng’s technique in the Kesanupalli-Challenger combination as discussed in Section IX.A.6. In particular, it would have been obvious for the *second processor* (sensor 204 functionality implemented on Challenger’s secure processor 26 in its TPM-based system) to be configured to implement Cheng’s technique and thus, for the second

processor to perform a secure backup. APPL-1003, ¶¶158-164. POSITA would have been motivated to configure the *second processor* to perform the backup process of Cheng because the secure backup is directed to the kind of data (user authentication information, electronic identity, etc.) that underlie security functions of the device, which POSITA would want to isolate from insecure processes and potential attacks, and the relevant records for backup are disposed in the secure storage accessible only by the second processor. *Id.* This was a common arrangement prior to the '512 patent, and would have been straightforward for POSITA to implement including widely practiced porting of code to a TPM environment. *Id.*; APPL-1019 (describing secure backup protocol elements from TCG standardization and implemented in a TPM), APPL-1017 (showing porting). As to limitation [1.7A], Cheng discloses a “biometrics-based authentication device,” and a *secure backup* of data of this first device by creating “backup file(s)” of the encrypted data, and providing these backup file(s) to a user service bureau, a *storage service*. APPL-1008, [0002] (“invention relates generally to portable authentication devices. More particularly, it relates to a new and useful system, method, and apparatus for **generating secure back up** of authentication information of a user and for restoring the authentication information back onto a portable authentication device.”), [0023]-[0028] (“a method for **creating a secure backup** of a portable biometrics-based authentication device includes the following steps: (a) obtaining a

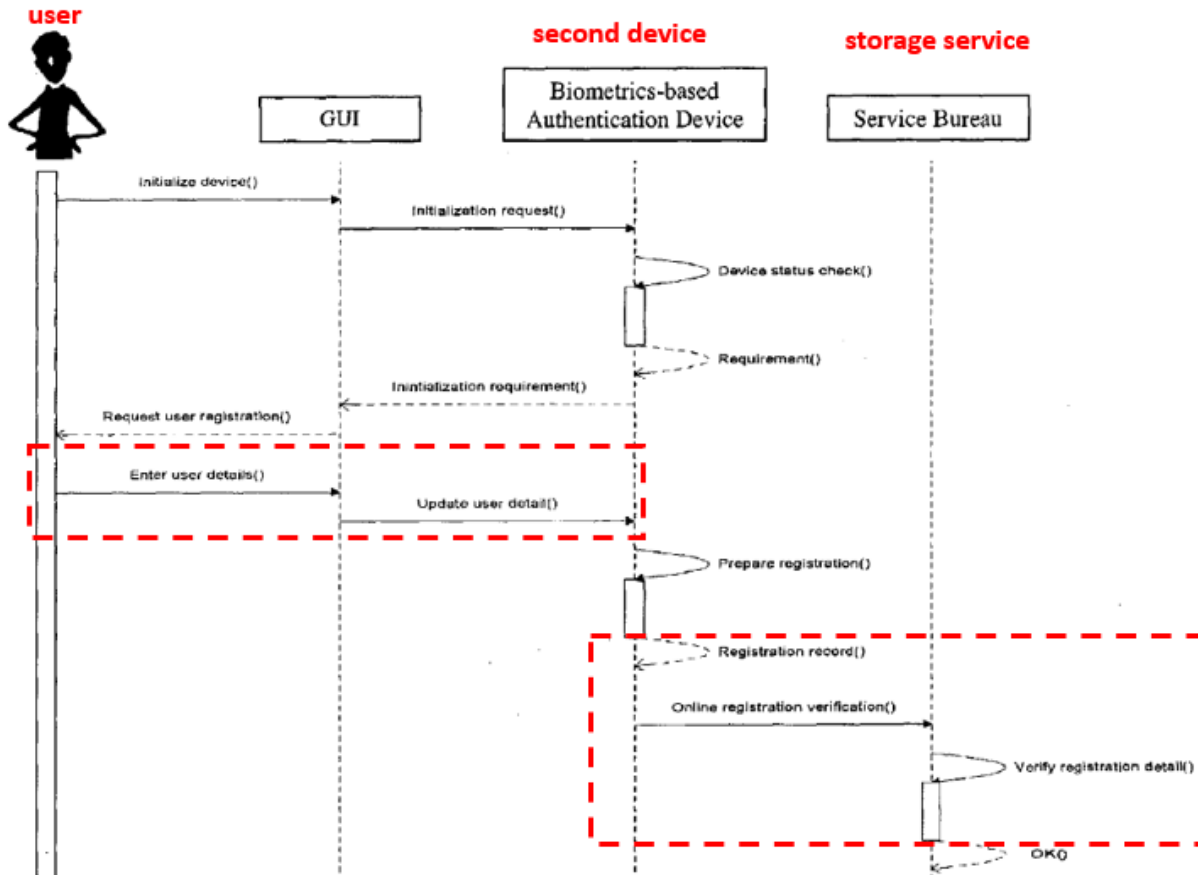
lower tier encryption key from a user service bureau; (b) enciphering lower tier authentication data using the lower tier encryption key, thereby **creating an encrypted lower tier backup file**; (c) obtaining an upper tier encryption key from the user service bureau; (d) enciphering upper tier authentication data using the upper tier encryption key, thereby **creating an encrypted upper tier backup file**; and (e) **storing the encrypted lower tier backup file and the encrypted upper tier backup file on a storage means.**”), [0029] (“The storage means could be, for instance, an online proprietary or Internet-based storage service, a remote server...[t]he user service bureau could be proprietary or Internet-based and could also provide the **storage service.**”)

Cheng describes exemplary types of data for backing-up, which includes user authentication information, such as “private keys, certificates, and other data held within the device” and “user’s biometrics information;” this is just the type of data included in Kesanupalli’s *record* (user credential and biometric template) as discussed above. APPL-1008, [0030]. *See also*, APPL-1008 [0007], [0008], FIGS. 3A, 3B. Thus, a predictable implementation of Cheng’s backup to a storage service is to securely backup Kesanupalli’s *record* for the reasons discussed in the motivation to combine above. Cheng’s backup is a *secure backup* as it creates a backup of the record (*e.g.*, backup file(s)) that is protected from unauthorized access (*e.g.*, by encryption) and transmits it to a storage service (*e.g.*, user service bureau).

APPL-1003, ¶¶165-169.

As to limitation [1.7B], Cheng describes embodiments where a restoration of the multiple-encrypted backup data onto a new device—a *second device*—is performed. To begin this restoration, Cheng’s backup procedure includes *register[ing] a second device associated with the user* with Cheng’s user service bureau, *the storage service*. APPL-1008, [0045]–[0047] (“1. A user’s biometrics-based authentication device becomes unavailable due to loss, damage, destruction, theft, etc. 2. The user obtains **a new** biometrics-based authentication **device**...3. The user **enrolls** the new biometrics-based authentication device with an enrollment service/user service bureau.”); [0031]–[0039] (including “The method of restoring authentication information of a user includes the following steps: (a) **verifying registration information of the user with a user service bureau**; (b) downloading an upper tier encryption key from the user service bureau...(d) restoring onto the portable biometric-based authentication device the upper tier authentication data from the decrypted upper tier backup file which includes the user’s backup biometrics data and any validation scripts, keys, and/or values...(h) restoring onto the portable biometrics-based authentication device the lower tier authentication data from the decrypted lower tier backup file.”) FIG. 4A, part of an “exemplary restore process” ([0013]) is illustrative of the second device registering (“**user details**”), which are provided to the service bureau, *the storage service*, in a

“registration verification.”



Cheng, FIG. 4A, portion, annotated

Thus, Cheng discloses a second device such as a user’s new device *is registered* with the storage service. APPL-1003, ¶¶170-171.

As to limitation [1.7C], Cheng describes data is *downloaded* from the service bureau, *storage service*, by the *second device*. APPL-1008, [0048] (“[t]he **new** biometrics-based authentication **device** establishes a secure connection with a user service bureau, begins the restore process and **downloads backup data from**

storage.”) *See also*, FIG. 4A, 4B, [0039], [0009] (“To restore the multiple-encrypted backup data onto a new [] device...upload the multiple-encrypted backup data onto the device.” *See* APPL-1003, ¶¶172-174.

As discussed above, POSITA would recognize that applying Cheng’s teachings to Kesanupalli’s record would be a predictable benefit to Kesanupalli/Challener system. In particular, backing up data including at least one record to a second device allows for the user to save resources (*e.g.*, time) in recreating the data in the record (*e.g.*, biometric template and/or user credential). APPL-1003, ¶174.

Thus, Kesanupalli, Challener and Cheng (in combination) render obvious this element, including each portion as delineated above.

[1.8] *a memory coupled to the first processor and configured to provide the first processor with instructions.*

Kesanupalli and Challener render obvious this limitation. APPL-1003, ¶¶176-180.

Kesanupalli’s system includes a main memory, a *memory*. APPL-1006, 10:26-47 (“Main **memory** is also usually included for storing and retrieving larger amounts of information such as data and software applications configured to perform functions according to the invention when executed by the central processing unit.”) POSITA would understand that the main memory of Kesanupalli’s system is *coupled to the first processor* and configured to provide the processor with

instructions such as those that execute the functions of Host PC 202 and sensor 204. APPL-1003, ¶¶177-178; APPL-1006, 5:59-66, 14:49-15:18.

In particular, the memory is coupled to the *first processor* as the main memory provides instructions for general processing functions. Challenger confirms a memory 36 is coupled to a general microprocessor 30—a *first processor*. APPL-1007, 5:26-40, 7:67-8:7 (“Program instructions implementing all or part of the present invention can be stored on and be accessible from a computer readable medium...examples of which include memory....”).

Thus, Kesanupalli and Challenger (in combination) render obvious “*a memory coupled to the first processor and configured to provide the first processor with instructions.*”

Therefore, claim 1 is obvious over Kesanupalli, Challenger, and Cheng.

8. Claim 2

[2.0] *The system recited in claim 1, wherein the storage service comprises a cloud storage service*

As explained above, Kesanupalli, Challenger and Cheng render obvious claim 1. Cheng renders obvious the further limitation of claim 2. APPL-1003, ¶¶181-183.

Cheng describes its backup process in terms of a storage service implemented as an “internet-based storage service.” APPL-1008, [0029]. POSITA would recognize that an internet-based storage service is *a cloud storage service*. APPL-1003, ¶182; APPL-1021 showing geographically dispersed services.

Thus, claim 2 is obvious over Kesanupalli, Challenger and Cheng.

9. Claim 3

[3.0] *The system recited in claim 1 wherein the second device is registered with the storage service at least in part by:*
connecting to the storage service; and
providing at least one of a user identifier or a credential to the storage service, wherein the user identifier comprises at least one of a username or an account number.

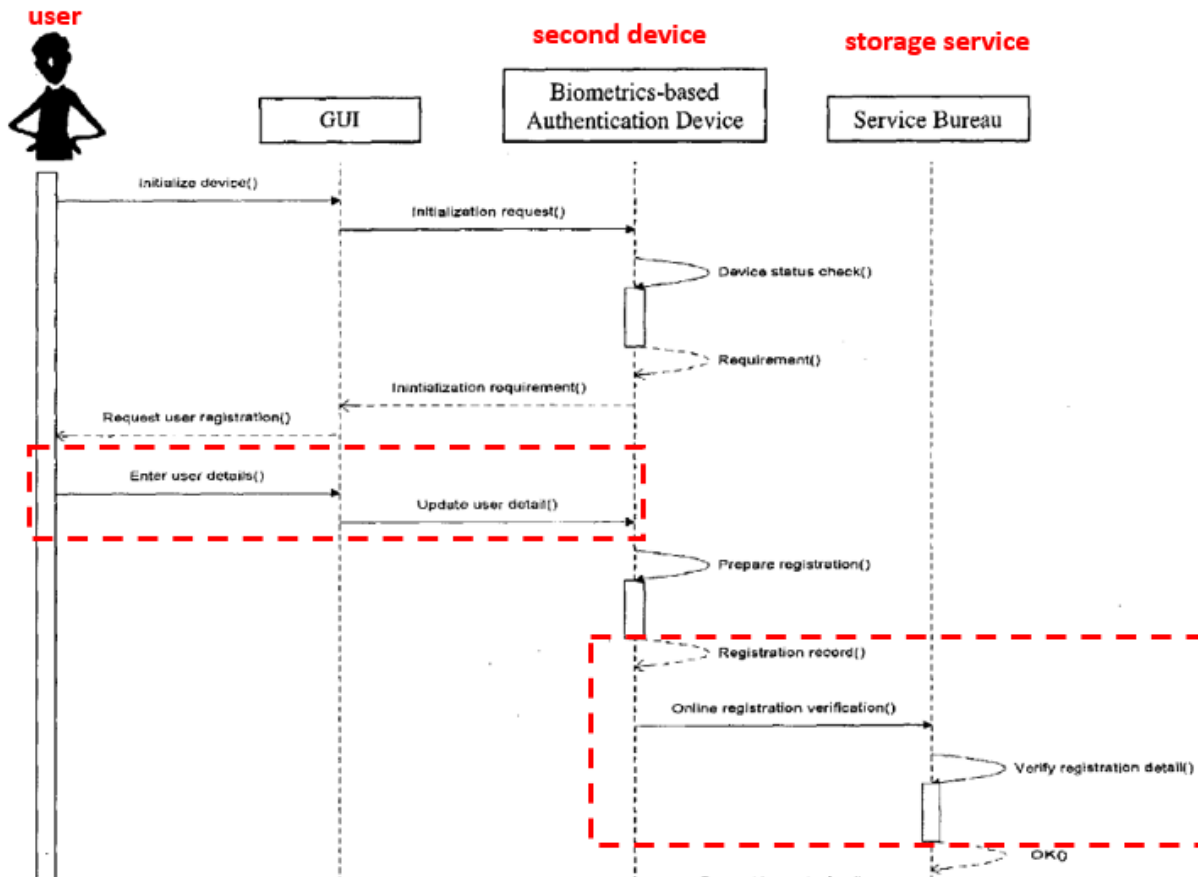
As explained above, Kesanupalli, Challenger and Cheng render obvious claim

1. Cheng discloses the further limitations of claim 3. APPL-1003, ¶¶184-188.

As discussed in limitation [1.6], Cheng describes registering the second device (*e.g.*, new or replacement device) with the storage service (referred to as user service bureau) and in doing so the second device *connect[s] to the storage service*. APPL-1008, [0048] (“The new biometrics-based authentication device establishes a secure **connection** with a user service bureau, begins the restore process and downloads backup data from storage”), FIG. 4A.

Cheng also discloses *providing at least one of a user identifier or a credential to the storage service*. FIG. 4A of Cheng shows a user providing the second device with “user detail(s),” from which the device forms a registration record that it sends through “Online registration verification” to the service bureau, the *storage service* (*See* limitation [1.6]). The service bureau then verifies the registration details. APPL-1008, [0032] (“**verifying registration information** of the user with a user service bureau” to begin its process of restoring backed-up data by enrolling the

second device. See also, APPL-1008, [0047].



Cheng, portion of FIG. 4A, annotated

POSITA would understand that “user details” that provide registration information are a *user identifier* and that a *username* or *account number* is a conventional and obvious example. APPL-1003, ¶187. A user identifier of a *username* or *account number* is a typical identifier used to enroll or register in any system. *Id.*, APPL-1006, 1:27-34 discussing “username” as a typical identifier. This is simply a standard piece of data for a service bureau, which is used by numerous users, to

identify the relevant data for subsequent transfer to the requesting device. APPL-1003, ¶187.

Therefore, claim 3 is obvious in light of Kesanupalli, Challener and Cheng.

10. Claim 4

[4.0] *The system recited in claim 1, wherein the record downloaded by the second device is encrypted.*

As explained above, Kesanupalli, Challener and Cheng render obvious claim

1. Kesanupalli and Cheng also render obvious the further limitations of claim 4.

APPL-1003, ¶¶189-191.

As discussed above in limitation [1.7], Cheng discloses a secure backup including a two-tier encryption of the record that is backed-up. Cheng continues to describe restoring, which is downloading, the record on the second device where the *encrypted* record is downloaded by the second device (*e.g.*, a new user device). APPL-1008, [0009] (“To **restore** the **multiple-encrypted backup data** onto a **new** biometrics-based authentication **device**, the user first needs to enroll the relevant biometric in the new device and **upload the multiple-encrypted backup data onto the device**, then contact the corresponding user service bureau to obtain an access clearance to the encrypted lower and upper tier encryption keys.”)

Therefore, claim 4 is obvious in light of Kesanupalli, Challener and Cheng.

11. Claim 5

[5.0] *The system recited in claim 4, wherein the encrypted record is stored to an insecure storage associated with the second device.*

As explained at [4.0], Kesanupalli, Challener and Cheng render obvious claim 4. The same combination renders obvious the further limitation of claim 5. APPL-1003, ¶¶192-196.

The '512 patent does not define “insecure storage” but states “[u]sers (and applications) can read from and write to the insecure storage area.” APPL-1001, 4:4-5. Continuing from claim [4.0], as Cheng teaches downloading a record protected under Cheng’s two-tier encryption structure, POSITA would have stored the received (and two-tier encrypted) record in an *insecure storage* of the second device. APPL-1003, ¶¶193-195.

As discussed above with reference to claim 1, the system of Kesanupalli implemented on the architecture of Challener, includes a general portion (PC 202) separate from a security portion. *See* Section IX.A.4. Challener illustrates a general processing portion includes a storage portion suitable for storing downloaded, encrypted data. APPL-1007, 5:26-36, FIG. 1, storage device 36, 5:26-32 (“A storage device 36, such as a hard disk drive, is also typically included to store data and applications to be used by the system 10. In the present invention, applications such as security applications to be loaded into processor 26, as well as other applications used by secure processor 26 and general microprocessor 30, can be stored securely

on storage device 36 **using encryption** and other security methods.”) POSITA understand that storage device 36 is insecure storage at least because it is accessible by multiple components. APPL-1003, ¶194; APPL-1007, FIG. 1, 5:26-40. Additionally, to the extent that the ’512 patent describes storage as “secure” or “insecure” this is merely a choice of two types of memory according to their established functions and with predictable tradeoffs. APPL-1003, ¶195, *see, KSR Int’l. Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

Therefore, claim 5 is obvious over Kesanupalli, Challener and Cheng.

12. Claim 6

[6.0] *The system recited in claim 4, wherein the second device is configured to decrypt the downloaded record and store the decrypted record to a secure storage associated with the second device.*

As explained at [4.0], Kesanupalli, Challener and Cheng render obvious claim 4. The same combination renders obvious the further limitations of claim 6. APPL-1003, ¶¶197-200.

First, Cheng discloses that the *second device is configured to decrypt the downloaded record*. APPL-1008, [0009] (“To restore the multiple-encrypted backup data onto a **new** biometrics-based authentication **device**...The device first requests the upper tier data decryption key from the user service bureau server to **decipher the encrypted upper tier data**...**Once the lower tier decryption key is received, the lower tier data is deciphered and stored in the device.** This

completes the restore process.”), FIGS. 4A, 4B.

After decryption of the downloaded record, POSITA would *store the decrypted record* (decrypted according to Cheng’s two-tier decryption) *[in] a secure storage associated with the second device* as taught in Kesanupalli and Challener. APPL-1003, ¶199. Kesanupalli and Challener each suggest storing personal data in a *secure storage*. APPL-1006, 6:45-48; APPL-1007, 4:57-5:9. Further, POSITA would have had reason to place data, decrypted with respect to the two-tiered encryption of Cheng, in a *secure storage* that is protected from unauthorized access to prevent “identity theft and/or unwanted intruders.” APPL-1003, ¶199; APPL-1008, [0003].

Therefore, claim 6 is obvious over Kesanupalli, Challener and Cheng.

13. Claim 10

[10.0] *The system recited in claim 1, wherein performing the cryptographic operation comprises decrypting the record.*

As explained above, Kesanupalli, Challener and Cheng render obvious claim 1. Kesanupalli renders obvious the further limitation of claim 10. APPL-1003, ¶¶201-203.

Kesanupalli as implemented on the architecture of Challener discloses a *second processor* configured to *perform a cryptographic operation* as discussed above in limitation [1.5], which illustrates *cryptographic operation* is *decrypting* the record. APPL-1003, ¶202, 42-47; APPL-1006, 6:31-49; APPL-1007, 4:24-36.

Thus, claim 10 is obvious in light of Kesanupalli, Challener and Cheng.

14. Claims 11–16 and 20

Claims 11-16 are obvious over Kesanupalli, Challener and Cheng. APPL-1003, ¶¶204-207. The limitations of independent claim 11, except limitation [11.0], the preamble, are substantively identical to limitations of claims already addressed above, as correlated in the table below:

Claim 11 Limitation	Corresponding Claim Limitation of Claim 1 illustrating that the limitation of Claim 11 is disclosed in Kesanupalli, Challener and Cheng
[11.1] <i>based at least in part on a request associated with a user to access an external resource, establishing, by a first processor of a first device, a secure connection with the external resource; and communicating with a second processor using a restricted interface,</i>	[1.1A], [1.1B], [1.1C]
[11.2] <i>wherein the second processor is configured to: receive a biometric input from a sensor, 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</i>	[1.2]
[11.3] <i>access a record stored in a secure storage, wherein the record is associated at least with the external resource;</i>	[1.3]

[11.4] <i>retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;</i>	[1.4]
[11.5] <i>perform a cryptographic operation;</i>	[1.5]
[11.6] <i>in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, 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 at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and</i>	[1.6] including [1.6A], [1.6B]
[11.7] <i>perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device</i>	[1.7] including [1.7A], [1.7B], [1.7C]

[11.0] *A method, comprising:*

To the extent the preamble is limiting, Kesanupalli and Challener render it obvious. The citations to Kesanupalli, Challener and Cheng above apply to a *system* as in claim 1 and also to a *method*. APPL-1003, ¶205; APPL-1006, 2:30-38 (“The systems and **methods** described herein relate to biometric authentication of users.”); APPL-1007, Abstract (“Method and apparatus for enabling applications on security

processors of computer systems.”); APPL-1008, Abstract (“it relates to a new and useful system, method and apparatus for generating secure back up of authentication information of a user and restoring the authentication information back onto a portable authenticated device.”)

Thus, claim 11 is obvious in light of Kesanupalli, Challener and Cheng for at least the reasons detailed above relative to claim 1.

Dependent claims 12–16 and 20 are substantively identical to claims already addressed above, as correlated in the table below but depend from the method claim 11. The combination of Kesanupalli, Challener, and Cheng renders obvious these claims for the same reasons discussed above with respect to claim 11 and the corresponding claims in of the table. APPL-1003, ¶207.

Claim	Corresponding Claim
[12]	[2]
[13]	[3]
[14]	[4]
[15]	[6]
[16]	[5]
[20]	[10]

15. Claim 21

Claim 21 is obvious over Kesanupalli, Challener and Cheng. APPL-1003, ¶¶208-211. The limitations of claim 21, except the preamble of limitation [21.0],

are substantively identical to limitations of claim 1 already addressed above, as correlated in the table below:

Claim 21 Limitation	Corresponding Claim Limitation of claim 1 illustrating that the limitation of claim 21 is disclosed in Kesanupalli, Challenger and Cheng
[21.1] <i>based at least in part on a request associated with a user to access an external resource, establishing, by a first processor of a first device, a secure connection with the external resource; and communicating with a second processor using a restricted interface,</i>	[1.1A], [1.1B], [1.1C]
[21.2] <i>wherein the second processor is configured to: receive a biometric input from a sensor, 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</i>	[1.2]
[21.3] <i>access a record stored in a secure storage, wherein the record is associated at least with the external resource;</i>	[1.3]
[21.4] <i>retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;</i>	[1.4]
[21.5] <i>perform a cryptographic operation;</i>	[1.5]
[21.6] <i>in response to determining that there is a match between the biometric input and a stored biometric template accessed by the second processor, facilitate a login of the user to the external resource at least in part by transmitting,</i>	[1.6]

<i>via the established connection, output based at least in part on the at least one of the password, the cryptographic key, or the cookie retrieved from the record, and wherein the user is logged in to the external resource based at least in part on the output; and</i>	
<i>[21.7] perform a secure backup of the record to a storage service, wherein a second device associated with the user is registered with the storage service, and wherein the record is downloaded from the storage service by the second device.</i>	[1.7]

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

To the extent the preamble is limiting, Kesanupalli and Challener render it obvious. APPL-1003, ¶¶209-210.

The citations to Kesanupalli, Challener and Cheng above apply to a *system*, 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. *Id.*; 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. Challener confirms what was well-understood by POSITA, that its first and second processors perform the tasks detailed by executing

instructions comprised in *computer program product embodied in a non-transitory computer readable storage medium*. APPL-1007, 7:64-8:7; APPL-1003, ¶210.

Thus, claim 21 is obvious over Kesanupalli, Challenger and Cheng.

X. DISCRETIONARY DENIAL IS NOT WARRANTED

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

A. The *Fintiv*⁴ factors favor institution.

Denial would be improper based on factors in *Apple v. Fintiv*, IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020) (precedential). Patent Owner asserted the '512 patent against Apple in WDTX-1-23-cv-00324 (“the Parallel District Court Proceeding”). *See* Section II.B.

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

⁴ Apart from Apple’s showing that *Fintiv* favors institution, the *Fintiv* framework should not be followed because it is legally invalid. The framework (1) exceeds the Director’s authority, (2) is arbitrary and capricious, and (3) was adopted without notice-and-comment rulemaking.

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

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

stipulates that, if the Board institutes trial, it will not pursue the same grounds raised in this Petition in the Parallel District Court Litigation. *See Sand Revolution II, LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020). The stipulation reduces any overlap and mitigates concerns of duplicative efforts or potentially conflicting decisions.

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

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

B. The Board should not deny under General Plastic

As indicated in Section II, the '512 patent has been involved a prior IPR proceeding, *Samsung Elec. Co., LTD v. RightQuestion, LLC*, IPR2022-00251 (the “Samsung IPR”). As shown below, *General Plastic* factors 1-5 each weigh in favor of institution. *General Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (Sept. 6, 2017) (precedential).

- Factor 1: Petitioner has not previously filed any IPR petition challenging any claim of the '512 patent. Thus, factor 1 weighs in favor of institution. Petitioner is unrelated to Samsung, and Petitioner has had no involvement in the Samsung IPR. Petitioner was never a “co-defendant” with Samsung. None of the “relationship” concerns set

forth in *Valve Corp. v. Elec. Scripting Prods., Inc.*, IPR2019-0062, Paper 11 (April 2, 2019) (precedential) are present here.

- Factor 2: Petitioner was served with the infringement complaint on April 4, 2023. The Samsung IPR was filed December 1, 2021. Petitioner did not know of—and had no reason to search for—the prior art cited in this Petition until after it was served, over 16 months after the filing of the Samsung IPR. Factor 2 weighs in favor of institution.
- Factor 3: To the extent Petitioner “received” Patent Owner’s preliminary response or the Board’s decision denying institution in the Samsung IPR because these documents were publicly available, this fact is negated by Petitioner being charged with infringement after the Board denied institution of the Samsung IPR. Factor 3 is neutral.
- Factor 4: After being served on April 4, 2023 and by about August 2023, Petitioner had completed prior art searches and began to develop the prior art grounds raised in this Petition. This Petition is filed more than 3 months before the statutory bar. Factor 4 weighs in favor of institution or is, at worst, neutral.
- Factor 5: Petitioner filed this Petition because the ’512 patent was asserted against Petitioner. The time between filing of this Petition and filing of the Samsung IPR petition is based on the fact the Petitioner

was served on April 4, 2023, sixteen (16) months after the Samsung IPR petition. Factor 5 favors institution.

- Factors 6 and 7 favor institution. No other proceeding involving the '512 patent is before the Office. Neither finite resources of the Board nor the Board's ability to issue a final written decision within the statutory time period are impacted by any other proceeding before the Office.

Thus, Samsung IPR factors 1-2 and 4-7 weigh in favor of institution, while factor 3 is neutral. The Board should not exercise its discretion to deny institution.

C. *Advanced Bionics* Test Favors Institution.

In determining whether to institute an IPR, the Board may consider whether “the same or substantially the same prior art or arguments previously were presented to the Office.” §325(d); *Advanced Bionics, LLC v. MED-EL Elektromedizinische Geräte GmbH*, IPR2019-01469, Paper 6, 7 (PTAB Feb. 13, 2020).

Relative to the first prong of *Advanced Bionics*, Petitioner acknowledges that *another* Kesanupalli reference was “previously presented to the Office.” More specifically, the Samsung IPR alleged obviousness based on Johansson in view of U.S. Patent Pub. 2011/0138450, naming Kesanupalli. *See Samsung*, IPR2022-00251, Paper 17, 10. The Kesanupalli '666 patent relied upon herein is not the Kesanupalli '450 publication (or counterpart thereof), although there is overlapping

disclosure. However, neither Challenger nor Cheng is similar—let alone cumulative—to Johansson, or any reference that was before the Board. Moreover, none of Petitioner’s references were before the Office during prosecution. Therefore, under the *first prong*, neither substantially the same art nor substantially the arguments were presented to the Office. *See Thorne Research, Inc. v. Trustees of Dartmouth College*, IPR2021-00491, Paper 18 at 7-9 (PTAB Aug. 12, 2021).

Under the *second prong* and even allowing for overlap between Kesanupalli disclosures, the Office “erred in a manner material to the patentability of challenged claims.” *See Advanced Bionics*, Paper 6 at 8, 10. First, the Board did not substantively consider the teachings of the Kesanupalli ’666 patent (APPL-1006) presented here, let alone those teachings in view of Challenger (restricted interface between processors) and Cheng (secure backup). Instead, the Board denied institution after finding that the prior petition failed to adequately support its contentions—without substantively evaluating even the teachings of the Kesanupalli ’450. *See* IPR2022-00251, Paper 17, 23-26 (“...constrained by the Petition, we are not persuaded that the cited evidence adequately supports Petitioner’s contention that Johansson, Kesanupalli [’450 publication], or the combination thereof teaches a “restricted interface” between processors”). Accordingly, the Board never reached (and therefore substantively overlooked) any disclosure of Kesanupalli [’450 publication] that could be said to overlap with the Kesanupalli ’666 patent relied

upon here. Thus, no Kesanupalli reference was “extensively evaluated for the same purposes” that the Petitioner now relies upon Kesanupalli ’666 patent in this Petition. *See Continental Automotive Systems, Inc. v. Horizon Global Americas Inc.*, IPR2021-00322, Paper 7, 19 (PTAB May 28, 2021).

Furthermore, neither the Challenger nor Cheng reference was even before the Board. This is notable because, as explained here (*see* Section IX.A.7, limitation [1.1C]), Challenger describes the “restricted interface” between processors that the Board found lacking in the Samsung Petition’s explanation of its Johansson and Kesanupalli [’450 publication] ground. *See* IPR2022-00251, Paper 17, 16. Likewise, as explained here (*see* Section IX.A.7, limitations [1.7A-C]), Cheng discloses the “secure backup” that the Board in found lacking in the Samsung Petition’s explanation of its Shaw-based ground and never addressed relative to the Samsung Petition’s Johansson and Kesanupalli [’450 publication] ground. *See* IPR2022-00251, Paper 17, 38, 23-26. Accordingly, these additional references and prior art teachings of “restricted interface” and “secure backup” were, at best, overlooked. Moreover, during prosecution, the Examiner cited absence of prior art teaching of “secure backup” in connection with allowance. For each of the foregoing reasons, the Office overlooked specific teachings in a manner that demonstrates material error relative to the Kesanupalli/Challenger/Cheng ground advanced in this Petition.

XI. CONCLUSION

Petitioner has established a reasonable likelihood that Challenged Claims of the '512 patent are unpatentable, and requests institution of *inter partes* review.

Respectfully submitted,

Dated: January 19, 2024

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

XII. CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. §42.24, the undersigned attorney for Petitioner declares that the argument section of this Petition (Sections I and III–XI) has 13,959 (less than 14,000) words, according to the word count tool in Microsoft Word™.

/David W. O'Brien/

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

CERTIFICATE OF SERVICE

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

Date of service January 19, 2024

Manner of service FEDERAL EXPRESS

Documents served Petition for *Inter Partes* Review, including Exhibit List;
Exhibits APPL-1001–APPL-1004, APPL-1006–APPL-
1009, APPL-1012–APPL-1028

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

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