

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

**PETITIONER'S REPLY TO
PATENT OWNER'S RESPONSE**

TABLE OF CONTENTS

I.	GROUND 1: KESANUPALLI, CHALLENGER AND CHENG RENDER THE CHALLENGED CLAIMS OBVIOUS	1
A.	PO misapplies the framework of obviousness analysis with respect to a POSITA	2
B.	PO mischaracterizes Kesanupalli’s goals.....	5
C.	PO misapplies the obviousness framework with respect to combining prior art teachings.....	9
D.	Kesanupalli is ready for improvement based on Challenger’s TPM-style architecture.....	11
1.	Tradeoffs or adoption of TPM do not preclude Challenger’s combination with Kesanupalli	14
E.	The <i>second processor</i> of Kesanupalli-Challenger is configured to “perform a secure backup of the record to a storage service” when considered in combination with Cheng’s backup technique.....	16
1.	PO does not rebut the Petition and accompanying expert testimony supporting obviousness of the claims that “perform a secure backup of the record to a storage service”	17
2.	TPM’s restricted access does not mean no interaction.....	20
3.	’512 patent’s backup technique provides for the <i>second processor</i> communicating with the <i>first processor</i>	21
4.	Secure backup of data on a user device to a storage service (cloud storage service) requires interim components	24
F.	Additional claim arguments	25
1.	Dependent Claims 2 and 12 are unpatentable over the Kesanupalli-Challenger-Cheng combination.....	25
2.	Independent Claims 11 and 21 are unpatentable over the Kesanupalli-Challenger-Cheng combination.....	26
II.	CONCLUSION.....	26
	CERTIFICATE OF WORD COUNT	27

CERTIFICATE OF SERVICE 28

PETITIONER'S EXHIBIT LIST

Updated: January 16, 2026

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, Authentication, Handbook of Computer Networks, Volume 3, Part 2, pp. 570-580, John Wiley and Sons, 2008. Ed. Hossein Bidgoli.
APPL-1013	IBM Introducing Fingerprint Reader Into Laptop. Jack Germain. 2004 at https://www.technewsworld.com/story/ibm-introducing-fingerprint-reader-into-laptop-37017.html (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, TPM Key Backup and Recovery For Trusted Platforms, 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, Carbyne Biometrics v. Apple, Inc., 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, Carbyne Biometrics, LLC v. Apple Inc., WDTX-1:23-cv-00324 (July 14, 2023)
APPL-1029	Sotera Stipulation dated April 17, 2024
(New) APPL-1030	Supplemental Declaration of Dr. Patrick McDaniel (“McDaniel Suppl. Decl.”)

(New) APPL-1031	Deposition transcript of Dr. Michael Goodrich (January 8, 2025)
(New) APPL-1032	Introduction of Computer Security, Michael T. Goodrich & Roberto Tamassia, Table of Contents, 2011
(New) APPL-1033	Techradar, Lenovo ThinkPad T60p review, Tech staff, May 4, 2008 (https://www.techradar.com/reviews/pc-mac/laptops-portable-pcs/laptops-and-netbooks/lenovo-thinkpad-t60p-305039/review), retrieved January 16, 2025 from archive.org, October 8, 2009 capture
(New) APPL-1034	Laptop Mag, Lenovo ThinkPad R500 Review, Jamie Bsals, August 20, 2008 (https://www.laptopmag.com/reviews/laptops/lenovo-thinkpad-r500), retrieved January 8, 2025
(New) APPL-1035	Intel Integrated TPM (Trusted Platform Module) for Windows XP (SP2) - ThinkPad R400, R500, T400, T400s, T500, W500, W700, W700ds, X2[], X200a, X200 Tablet, X301 (https://pcsupport.lenovo.com/us/en/downloads/ds001667), retrieved January 8, 2025

I. GROUND 1: KESANUPALLI, CHALLENGER AND CHENG RENDER THE CHALLENGED CLAIMS OBVIOUS

Claims 1-6, 10-16 and 20-21 are rendered obvious by Kesanupalli in view of Challenger and Cheng. In particular, in the Petition, Ground 1 shows application of Challenger's teachings of a TPM-type security architecture to Kesanupalli's techniques to provide a security processor (*a second processor*) in a secure portion communicating with a general processor (*a first processor*) in a standard portion with API-mediated interfaces of the second processor in between. *See* Petition, pp. 18-24, 27-54, 59-60. Ground 1 further applies Cheng's teachings of *a secure backup* of user authentication data, which is just like the data (biometric information and credentials for user authentication) that is securely stored and accessible by the *second processor* of the Kesanupalli-Challenger architecture (Kesanupalli's sensor functionality implemented on Challenger's secure processor). *See* Petition, pp. 24-27, 54-59 citing APPL-1008, [0030].

In its Patent Owner's Response (POR), Patent Owner's (PO) arguments regarding a supposed lack of motivation to combine the teachings of the Challenger and Kesanupalli references fail because they rely on irrelevant speculation as to the decisions of one person—Mr. Ramesh Kesanupalli—regarding what to include in a patent disclosure and ignore the motivation to combine offered in the Petition by focusing on a legally irrelevant mischaracterization that Kesanupalli's "concerns" were limited to a social engineering problem. Additionally, PO's arguments

regarding a lack of capability of the *second processor* in the Kesanupalli-Challener combination to perform Cheng's backup technique are incorrect and mischaracterize what is disclosed (and claimed) in U.S. Patent 10,929,512 ("the '512 patent").

A. PO misapplies the framework of obviousness analysis with respect to a POSITA

The Petition and accompanying declaration of Dr. McDaniel set forth the requisite factors for obviousness including the level of a person having ordinary skill in the art (POSITA) and the reasons why a POSITA, at the time of the invention, would have been motivated to combine Challener's teaching of a trusted platform module (TPM)-type security architecture with Kesanupalli's techniques for authentication using biometric information. PO does not rebut the legal or technological sufficiency of this evidence. Rather, PO conjures reasons that Mr. Ramesh Kesanupalli¹—the individual—did not include a "TPM" within the text of Kesanupalli—the patent—and argues that its conjured reasoning is determinative of non-obviousness. PO's reasoning is neither factually supported, nor legally relevant.

First, (pre-AIA) 35 U.S.C. §103(c) provides the statutory framework by which obviousness is to be determined and makes clear that it is an inquiry from the perspective of a POSITA. A POSITA is an imaginary person(s), a hypothetical legal

¹ Mr. Ramesh Kesanupalli is one of five inventors. APPL-1006, (75).

construct. The subjective decisions of Mr. Ramesh Kesanupalli (like those of Dr. Challenger), even if demonstrated unambiguously (and they are not), are not a stand-in for the legal construct of a POSITA.²

Second, PO's argument invites the Board to eviscerate the obviousness doctrine. PO attempts to disguise its over-reach by presenting its argument as "a unique opportunity" involving "unique facts." *See* POR, pp. 15-16. There is nothing "unique" about a patentability challenge involving "review [of] a reference from a contemporary POSITA." *See* POR, p. 15. Technical papers and patents are commonly, if not prevalently, attributed to authors/inventors having credentials that meet or exceed those of a POSITA. Should patentability be concluded based on what that author/inventor subjectively chose to include within his article/patent, only anticipatory challenges to patentability would remain. Statutory law and case law demand that is incorrect. "[I]n many cases a person of ordinary skill will be able to

² In Paper 10 the Board adopted Petitioner's POSITA standard "except for the language 'at least'[".] Paper 10, p. 18. Petitioner applies the standard as clarified by the Board. The analysis of the Petition remains the same, applying this clarified level of skill for a POSITA. APPL-1030, ¶9 (Dr. McDaniel explaining that his analysis in APPL-1003 remains the same).

fit the teachings of multiple patents together like pieces of a puzzle.” *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 420 (2007).

Third, *why* Mr. Ramesh Kesanupalli chose not to include a discussion of TPM within a patent application is unknown. PO's arguments (*see* POR, pp. 16-17) are simply unsupported conjecture.³ There may be any number of reasons that a standards-based TPM or numerous other well-known features of information security and security arrangements for protecting computers or other electronic devices are not expressly called out in the text of Kesanupalli.⁴ Not the least of these reasons is that Kesanupalli stems from a U.S. Patent application (Appl. 12/731,505). An inventor has reason and motivation to ensure that his patent application meets the enablement and written description requirements of U.S. patent law with respect to his claimed invention. There is no reason, no necessity and no expectation that a patent survey all available related features or describe further combinations beyond the invention claimed therein.

³ Dr. Goodrich's deposition shows he does not personally know Mr. Ramesh Kesanupalli (nor Inventor David Challener). *See* APPL-1031, pp. 7, 68-69.

⁴ *See* APPL-1030, ¶¶10-13 (discussing reasons why a standards-based TPM may not be detailed and discussing POSITA.)

B. PO mischaracterizes Kesanupalli's goals

As the Petition explained, “Kesanupalli...is directed to a secure authentication system that uses biometric information to ‘provide[] a more secure authentication of the user than commonly used password-based methods and systems.’” Petition, p. 10 (citing APPL-1006, (54), 1:59-62, APPL-1003, ¶¶61-76). To protect the user’s sensitive information, “[t]he fingerprint template and user credentials are then stored in a secure storage of the user’s device.” Petition, pp. 10-11 (citing APPL-1006, 3:46-47, 5:61-6:49, 8:29-53); Petition, pp. 11-12 (citing APPL-1006, Fig. 2 (“secure storage”)). However, PO argues that “Kesanupalli [the patent] is only concerned with [a problem of] social engineering” attacks (*see* POR, p. 25) and posits that because a TPM is not narrowly targeted to that same problem, the combination fails.⁵ First, this is a mischaracterization of Kesanupalli, and second, as discussed in

⁵ PO’s distinction between an attacker’s *initial* strategy is untenable as these attacks are often interrelated and social engineering attacks are often used as a precursor to other attacks (e.g., to deploy malware). APPL-1030, ¶21. This is one reason why a POSITA does not approach security with a goal of mitigating just one type of attack and why Kesanupalli addresses device security features in implementing its authentication techniques. APPL-1030, ¶¶22, 31 (explaining defense in depth and citing APPL-1032).

Section I.C, this is not the proper framework in which to determine obviousness of the claims of the '512 patent.

Kesanupalli's teachings are not constrained to *only* mitigating social engineering attacks. PO recognizes that Kesanupalli begins by recognizing that typical authentication systems use passwords, which are at risk for attacks "including 'phishing attacks' and 'social engineering attacks.'" *See* POR, p. 6 (citing APPL-1006, 1:35-37). However, these two recognized risks—phishing and social engineering attacks—to which PO attempts to constrain all of Kesanupalli's teachings, appear once in its background discussion. And even here, the entirety of the cited sentence shows that Kesanupalli's teachings are not so limited: "Although passwords are commonly used to authenticate users, **passwords** are subject to **various attacks, such as** phishing attacks, social engineering attacks, dictionary attacks and the like." APPL-1006, 1:35-38 (emphasis added).⁶ There is no requirement (explicit or implicit) in Kesanupalli that its authentication systems and

⁶ Notably, the explicitly mentioned "dictionary attacks," omitted by the POR's quotation and are not social engineering attacks that trick a user, but a different security risk mitigated by strong passwords. APPL-1031, p. 26 ("Q: So does dictionary attacks trick people as social engineering did? A: No, not usually..."). *See also*, APPL-1030, ¶19.

methods only address social engineering attacks. APPL-1030, ¶14. Rather, Kesanupalli's specification broadly discusses authentication systems and methods without constraining their purpose and claims these systems and methods without such a limitation. *See* APPL-1006, 10:47-54, 11:5-38. Kesanupalli discloses numerous security features not driven solely by a concern for social engineering attacks. APPL-1030, ¶¶14-22 (Dr. McDaniel describing Kesanupalli's use of cryptographically secured communications, secure storage, digitally-signed code, and other features).

While Kesanupalli facilitates the use of secure, complex passwords by freeing a user from remembering those complex passwords, it does so by storing a copy of the passwords (or other credentials) and biometric information. In doing so, Kesanupalli mitigates one set of risks—weak passwords and social engineering attack risk. But another risk comes to the fore—breach of the device with the password biometric information store(s). APPL-1030, ¶15 (highlighting that stored passwords/keys/biometric information become targets).

This is one reason Kesanupalli describes numerous specific security features that are not focused exclusively on social engineering attacks or on promoting stronger passwords. Rather, these security features focus on protecting passwords, other credentials such as cryptographic keys, and biometric information from compromise while held in its device and during communication. For example,

Kesanupalli discusses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor, implementing strong cryptographic algorithms in its hardware and/or software, strengthening security by biometric sensor unique identifiers (ID), using cryptography features of secure keys and hashes, and so on. APPL-1030, ¶¶14-22 (citing APPL-1006, 1:28-30, 6:39-42, 4:12-23, 4:64-5:33).⁷ Further, Kesanupalli generally discusses providing “secure transactions,” “secure application,” and “secure communication,” with no implication that these are “secure” *only* with respect to social engineering attacks. APPL-1030, ¶17 (citing APPL-1006, 5:53-58, 6:15-17, 6:39-42).⁸ In perhaps a plainest example, Kesanupalli provides its storage for biometric data and credentials in “a **secure** storage device.” APPL-1006, 3:46-

⁷ See also, APPL-1031, pp. 40-42 discussing cryptographic hash functions are for “confidentiality”, use of digital signatures (keys) for “integrity”, which confirms Dr. McDaniel’s discussion of APPL-1003, ¶¶45-47 (describing cryptography, including encryption and hash functions, as being “for a goal of protecting confidentiality and/or integrity (protecting against corruption) of data”).

⁸ See also, Ex. 2037 discussing Kesanupalli’s security feature of digitally signing and checking credentials and biometric components; APPL-1003, ¶18, 28-33 discussing same.

51, 6:6-10 (emphasis added). Thus, Kesanupalli is certainly concerned with breaches to its device—why else place the credentials in a “**secure** storage” of its architecture. *See* POR, p. 26. Any one of these features shows that Kesanupalli is concerned with security as a whole, including device security.

C. PO misapplies the obviousness framework with respect to combining prior art teachings

PO argues against the combination of Kesanupalli with Challenger, allegedly because Challenger's TPM-based architecture “would not have helped avoid social engineering attacks.” *See* POR, p. 20. PO provides no indication as to how this, even if true (which it is not as discussed above in Section I.B), would save its claims from being unpatentable.

First, the Petition shows that Kesanupalli, Challenger and Cheng are all analogous art to the '512 patent. Paper 2, pp. 22-23, 25. PO does not dispute this. When more than one prior art reference is used as the basis of an obviousness rejection, it is not required that the references share a common singular problem. *See Sanofi-Aventis Deutschland GmbH v. Mylan Pharms. Inc.*, 66 F.4th 1373, 1380 (Fed. Cir. 2023) and *Corephotonics, Ltd. v. Apple Inc.*, 84 F.4th 990, 1007 (Fed. Cir. 2023).

Second, Kesanupalli's teachings are neither limited to the problem of social engineering attacks, nor would any recognition of a particular problem by Kesanupalli constrain the obviousness inquiry to solving just that particular problem.

Rather, the inquiry is from the perspective of a POSITA with all his relevant knowledge as “a person of ordinary creativity, not an automaton.” *KSR*, 550 U.S. at 421 (discussing exemplary motivations). PO’s attempt to confine an obviousness inquiry to a particular problem has been squarely rejected by the Supreme Court. *KSR*, 550 U.S. at 404.

Third, social engineering attacks are but one type of security threat related to the information security and access controls that are used to protect computers or other electronic devices. They do not exist in a vacuum. A POSITA would have recognized that social engineering is often an attack vector for intrusions that seek sensitive personally information such as passwords and security keys. APPL-1030, ¶22. Moreover, POSITA would have readily recognized that addressing system vulnerabilities cannot be constrained to just one type, or stage, of attack and still provide a secure system. *See* APPL-1030, ¶¶22, 31-33 (discussing defense in depth); APPL-1031, pp. 37-38 discussing “the concept of computer security is wrapped up into a number of other sub-concept” including “confidentiality, integrity, and availability” and “assurance, authenticity, and anonymity”), pp. 13-14, 71-72 discussing textbook use including APPL-1032. This is exactly the sort of flexible analysis required under *KSR*. *KSR*, 550 U.S. at 424 (“The proper question to have asked was whether a [person] of ordinary skill, facing the wide range of

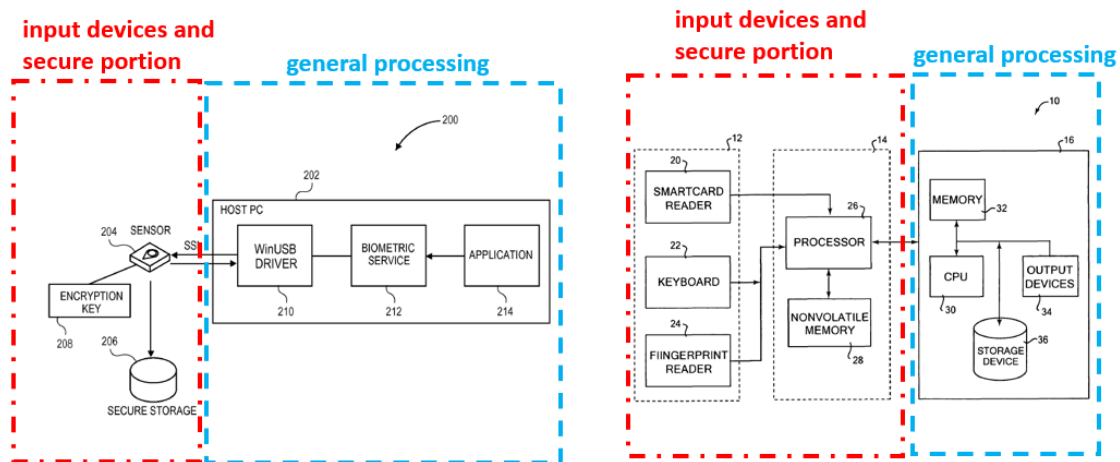
needs created by developments in the field of endeavor, would have seen a benefit to upgrading [the primary reference] with a [particular feature].”)

PO's attempt to limit a POSITA's perspective to only one type of attack is specious on its face. It is akin to arguing that daily transport of cash to the bank by armored car after verifying the identity of the driver would preclude any motivation to use a safe on premise or that anti-lock brakes obviate and render non-obvious the use of seatbelts and airbags.

D. Kesanupalli is ready for improvement based on Challenger's TPM-style architecture

The Petition, with reasoned analysis supported by evidence, showed that a POSITA would have been motivated to apply Challenger's teachings of a TPM-type security architecture (with its *first* and *second processor[s]* and API-mediated interfaces) in implementations of Kesanupalli's authentication techniques (with Cheng's backup). In particular, Challenger's secure processor 26—a *second processor*—implements a security architecture that includes API functions used in its communication with other components, including general microprocessor 30—a *first processor*. In particular, the security functions of Kesanupalli's sensor 204 are beneficially implemented using Challenger's specialized security processing circuitry such as illustrated by Challenger's security processor 26 and its restricted interfaces (to its storage and general processing) because a standards-based TPM architecture would provide support for many underlying cryptographic security services and

secure storage facilities and because using standards-based TPM architecture would have engendered trust among users and customers. Petition, pp. 18-24 citing APPL-1003, ¶¶83-84, 48-51. That is, it would have been obvious to implement the functions of the red-delineated portion of Kesanupalli using the processing, interfaces and storage elements of the red-delineated portion of Challenger's TPM-based architecture, which includes Challenger's API-mediated connections such as between the security processor (*second processor*) and the general processor (*first processor*), *i.e.*, a *restricted interface*. See also, APPL-1030, ¶¶28-35.



**Kesanupalli, FIG. 2 and Challenger, FIG. 1,
annotated and juxtaposed; see also Pet., p. 20, APPL-1003, ¶¶78-79**

Rather than address this combination, PO continues to incorrectly suggest that Kesanupalli was not concerned with device security (arguments that are legally flawed for the same reasons discussed above). In particular, PO and its expert Dr.

Goodrich each argue that Kesanupalli's architecture allows sensitive data in the form of biometric information and credentials to be handled by a browser extension (within Kesanupalli's blue-delineated portion above), which is executing on Kesanupalli's general processor. *See* POR, pp. 25-26. According to the POR, "[i]f the device was breached by a bad actor, this process [of Kesanupalli providing sensitive data in the browser extension] would make the credentials available to the bad actor." POR, p. 28; *see also*, POR, p. 26 discussing the bad actor of malware. The POR argues this security risk of its browser extension means Kesanupalli is concerned *only* with social engineering attacks, not attacks that breach the device. POR, pp. 26-28. This is flawed logic, as Kesanupalli is, in fact, concerned with malware risk and digitally signs its browser extensions to mitigate this risk. APPL-1030, ¶¶18, 28-35. Moreover, as discussed above, neither Kesanupalli itself, nor a POSITA's motivations, nor the framework of an obviousness analysis are so limited as to consider attacks from only one style of attacker or vector. Further, a POSITA would recognize that an architecture with security risks invites combining additional security features.⁹ Challenger's security architecture provides benefits to overall

⁹ The PO's theory of unmitigated risk is also unsupported attorney argument directly contradicted by PO's expert Dr. Goodrich. *See* Ex. 2037, ¶¶60, 57 ("Kesanupalli reference's system securely provides sensitive information to the application

security by securing data and cryptographic services that underly functionality performed by Kesanupalli. APPL-1030, ¶¶13, 29-35.

1. Tradeoffs or adoption of TPM do not preclude Challenger's combination with Kesanupalli

PO agrees that TPMs were “well known” and covered by published, international industry standards years before the '512 patent. POR, p. 11.¹⁰ PO however incorrectly argues that combining teachings related to TPMs would have been non-obvious because TPMs were not **required** in commercial products or “not on by default.” POR, pp. 12, 30. Market adoption rate is not a factor of obviousness. There were certainly commercial products that implemented TPMs prior to the earliest effective filing date of the '512 patent (December 2011). APPL-1030, ¶¶23-

processor executing the biometric browser extension” that is “digitally signed and validated at runtime...so malware cannot compromise credential information.”) Security features of Kesanupalli's browser extension are directed to a different portion of the architecture than Challenger's teachings. APPL-1030, ¶¶28-34 (explaining browser extension relative to TPM). And such security features are entirely consistent with a multi-faceted security approach. APPL-1030, ¶¶22, 28-34.

¹⁰ Ex. 2051 is a 2009 standard for TPMs by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

27 (citing APPL-1033, Lenovo ThinkPad T60p review *circa* 2008, describing “biometric fingerprint scanner...linked to a Trusted Platform Module (TPM) chip.”).

To the extent that PO alleges “compatibility issues” (*see* POR, p. 30) with respect to use of a TPM, PO’s alleged issues are not supported by any reasoned analysis, rather they devolve to a slow market adoption argument. APPL-1030, ¶35 (Dr. McDaniel disagreeing with supposed compatibility issues). That TPMs were covered by an adopted industry standard well before the ’512 patent effective filing date and, according to the PO itself, would be “required” shortly thereafter suggests a lack of compatibility hurdles. Ex. 2042, at 336, n. 3 (citing a Microsoft hardware certification requirements document from 2013 that announced the TPM requirement for future certifications); APPL-1030, ¶27 (Dr. McDaniel discussing that technology had to be well understand and widely used long before a company like Microsoft would require every one of their customers to have one). At bottom, PO provides no evidence as to *why* a TPM, much less Challenger’s architecture, is incompatible with Kesanupalli’s technique as it alleges; their compatibility is set forth in Petition and accompanying declaration. *See, e.g.*, Petition, pp. 18-24 citing APPL-1003, ¶¶74-84 including discussing the correspondence of general/secure processor portions, secure storage, and fingerprint readers in the teachings.

Further, PO’s arguments are again mischaracterizing what is required of obviousness. The Petition accompanied with Dr. McDaniel’s analysis showed that a

POSITA would have had reason and seen a benefit to applying Challenger's TPM-based architecture to perform the authentication techniques of Kesanupalli with a reasonable expectation of success. Petition, pp. 18-23. PO does not dispute the benefits of implementing a standards-based TPM architecture. Even if benefits are tempered by drawbacks such as lack of industry-wide adoption, this does not save it from obviousness. *See KSR*, 550 U.S. at 403.

E. The *second processor* of Kesanupalli-Challenger is configured to “perform a secure backup of the record to a storage service” when considered in combination with Cheng’s backup technique

The Petition (and accompanying evidentiary support) illustrated that it would have been obvious in light of Cheng to perform a *secure backup* because doing so was known in the art, convenient to the user, met a desire in the market, and was necessary for data recovery such as for a lost device. *See* Petition, pp. 25-27 citing APPL-1003, ¶¶50-55. *See also*, Petition, pp. 24-27, 54-59 citing APPL-1003, ¶¶70-73, 157-175. The PO does not rebut this.

The Petition (and accompanying evidentiary support) also showed a POSITA would particularly have configured the *second processor* to perform this *secure backup* because the *second processor* has exclusive access to the sensitive records; the backup involves security features, which are the purview of the *second processor*; and the *second processor* has the capabilities to performing such a *secure backup* (e.g., access to the record, encryption capabilities, executable instructions).

Petition, pp. 25-27, 54-56 citing APPL-1003, ¶¶85-91, 157-175. The PO also does not rebut this.

Rather, the PO argues that because the Kesanupalli-Challener architecture includes a communication flow between the *second processor* and the *first processor*, the *second processor* is not “configured to...perform a secure backup of the record to a storage service.” POR, p. 32-33. This is a mischaracterization of the record that shows it would have been obvious in light of Cheng's teachings to configure the *second processor* to perform the secure backup. Further, PO's suggestion that the *second processor* must be the sole actor involved in performing a secure backup to a storage service such as a cloud service is not what is described in the '512 patent or what would be understood by a POSITA.

1. PO does not rebut the Petition and accompanying expert testimony supporting obviousness of the claims that “*perform a secure backup of the record to a storage service*”

Again, the Petition set forth reasons to combine the backup technique of Cheng with Kesanupalli-Challener in its Section IX.A.5, and then detailed this combination including with respect to the role of the *second processor* in Section IX.A.7, element [1.7] including [1.7A], [1.7B], [1.7c]. Petition, pp. 24-27, 54-58. Notwithstanding the Petition's extensive discussion, as well as Dr. McDaniel's extensive, evidence-supported, technical explanation referred to therein that detailed the implementation of those teachings, the POR attempts to characterize the

Petitioner's analysis as "a single paragraph" devoid of consideration of "how the backup method would be added to the Sensor/TPM architecture." *See* POR, p. 35. This is a mischaracterization of the record, which describes how and why the backup method of Cheng would have been added to Kesanupalli-Challener with a reasonable expectation of success.

In particular, the Petition, supported by Dr. McDaniel, explained that a 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 (*e.g.*, user authentication information) that underlie security functions of the device, which a POSITA would want to isolate from insecure processes and potential attacks, and because the relevant records for backup are disposed in the secure storage accessible only by the *second processor*. *See* Petition, pp. 54-57 citing APPL-1003, ¶157 discussing applying Cheng's teachings of 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], [0007], [0023]-[0028]). The Petition is supported by Dr. McDaniel's testimony spanning paragraphs 157-175 of APPL-1003 providing specific implementation details. In particular, Dr. McDaniel discussed that "an import management function of TPM-based systems was commonly used for backup and recovery of TPM data" and provided an example of

APPL-1018 (an Infineon Whitepaper) that discussed such backup. APPL-1003, ¶160 (citing APPL-1018 p. 4, which advises backup of TPM by a centralized backup-server). And Dr. McDaniel went on to describe the process of porting code to the TPM to provide the configuration of the second processor to perform the backup. APPL-1003, ¶¶160-162. Furthermore, Cheng states an onboard microprocessor of the biometric-based authentication device performs the backup. APPL-1008, [0022]. *See* APPL-1003, ¶173, Petition, p. 59. This suggests to a POSITA that the processor that authenticates against stored biometric information—i.e., the *second processor*—also performs the backup. APPL-1003, ¶173, cited at Petition, p. 59. Cheng's disclosed secure backup technique includes security features of encrypting the data before transmission and a secure transmission to a storage service, thus ready for combination with Kesanupalli-Cheng and implementation by a secure portion of the architecture. *See* Petition, pp. 55-57 and APPL-1003, ¶¶158-169 describing Cheng's encryption (e.g., APPL-1008, [0023]-[0028]) and secure communication between the storage service and biometrics-based authentication device (APPL-1008, [0029]). *See also*, APPL-1030, ¶36 reiterating that the second processor of Kesanupalli-Challener architecture is configured to “*perform a secure backup of the record to a storage service*” when considered in combination with Cheng's backup.

PO does not rebut any of this analysis. PO's turning a blind eye does not erase the record. The Board recognized that the Petitioner's "evidence is sufficient to show that the combination would have worked for its intended purpose." Paper 10, p. 51. This remains unrebutted.

2. TPM's restricted access does not mean no interaction

The POR recognizes that the "TPM is restricted so as to keep its contents safe from unauthorized access." POR, p. 36. But a desire to preclude unauthorized access or to restrict access to the data does not preclude a TPM or the secure processor of a TPM-based architecture from performing a secure backup. Simply put, being restricted or preventing unauthorized access does not mean no interaction with the outside world. APPL-1030, ¶¶37-39 (Dr. McDaniel explaining that, in the '512 patent description, downstream components are along the propagation path of the second processor's secure backup to a storage service such as a cloud service). Instead, it means that outside access is restricted to authorized access, and it would be obvious to perform Cheng's backup technique from within the restricted interface provided by the second processor as it includes security features. *See* Petition, pp. 54-58, APPL-1003, ¶169 discussing security features such as Cheng's encryption and use of a secure connection to the storage service (APPL-1008, FIGS. 3A-3B, [0023]–[0029]). And such systems were known to have a reasonable expectation of success. APPL-1003, ¶160 (citing APPL-1018, p. 4 discussing back-up of TPM).

3. '512 patent's backup technique provides for the *second processor* communicating with the *first processor*

Contrary to the position in the POR, PO does not point to any disclosure in the '512 patent that requires the *second processor* to communicate directly with the outside world. The '512 patent discusses the first and second processor in the context of its FIG. 3, which is discussed beginning at column 3, line 66. *See* APPL-1031, pp. 34-35. Just like the Kesanupalli-Challener architecture, this portion of the '512 patent describes that users can interact with an insecure storage, which is associated with the fast processor 304 (*first processor*). And the fast processor (*first processor*) communicates with the dedicated processor/sensor (*second processor*), which controls access to the secure storage area 306. APPL-1001, 4:4-8 ("Users (and applications) can read from and write to the insecure storage area. **However, users cannot access the secure storage area, and the fast processor can only communicate** with the dedicated processor/sensor via a restricted API.") In terms of a backup process, the '512 patent describes that the sensitive data is within "an encrypted and authenticated container that can be stored on insecure storage, e.g., on the device, and also backed up (e.g., to a cloud storage service 140 or to an alternate form of external storage)." APPL-1001, 4:10-15. The encryption is

performed by the *second processor*. APPL-1001, 3:60-4:26.¹¹ This means that the backup process involves the record comprising sensitive data that, once encrypted by the *second processor*, is sent to the insecure storage accessible by the *first processor*. APPL-1030, ¶39. PO's expert agrees that the communication flow is between the *second processor* and the *first processor*.

Q. So is there communication between the processors 304 and 308 in figure 3?

A. If you're asking about the preferred embodiment of how -- what figure 3 is illustrating, that's discussed, for example, beginning in column 3, starting at line 66, and then continuing into column 4. And one of the disclosures begins at line 5. It says, "however, users cannot access the secure storage area, and the fast processor can only communicate with the dedicated processor/sensor via a restricted API."

Q. Is it correct that the dedicated processor sensor is 308?

¹¹ PO has agreed that secure backup includes encryption, which is performed by the second processor. See IPR2022-00251, POPR, p. 41 (citing '512 patent 3:60-4:26 and stating "[t]hese exemplary embodiments demonstrate that "performing a secure backup" first encrypts the data and then backs up the encrypted data to cloud storage or another storage service.")

A. Yes, ...

Q. So can a processor 304 communicate directly to the Internet?

[objection]

THE WITNESS: If by communicate directly with the Internet, you mean can that processor be used by a user to access an external resource across the Internet and establish a secure connection with that external source, the answer is yes.

Q. [] Can the user do the same with the processor 308?

A. No. As I read earlier, at line 5 of column 4, it states, "however, users cannot access the secure storage area, and the processor can only communicate with the dedicated processor/sensor via restricted API."

And then of course that -- it goes on in this passage to talk about how the secure processor can communicate with other entities, but then that is not the user doing that anymore. It's now the secure processor doing it in response to perhaps a communication through the restricted API.

APPL-1031, pp. 35-36.

Thus, PO's expert himself identifies the portion (col. 4) of the '512 patent that describes that backup of the record is provided from the secure storage accessible by the dedicated processor (*second processor*) to the insecure storage accessible by the fast processor (*first processor*), which, in turn, communicates it to cloud storage. APPL-1001, 4:19-23 ("Profiles and vaults can be updated while in secure storage; if this occurs, they are encrypted and MACed before being written back to the insecure storage, which may in turn propagate them to external backup storage."); APPL-1030, ¶39. Thus, PO's attempt to characterize the second processor as performing

the secure backup without any communication with the first processor is in conflict with its own patent's disclosure.¹² APPL-1030, ¶¶37-39.

**4. Secure backup of data on a user device to a storage service
(cloud storage service) requires interim components**

Finally, PO's argument devolves to requiring the *second processor* have an exclusive role in the *secure backup...to a storage service*, which is untenable. Performing a secure backup to a storage service such as a cloud storage service (claim 2) necessarily includes other components, including other processors outside of the *second processor*. APPL-1030, ¶¶37-41. Fig. 1 of the '512 patent is illustrative of the communication path between a user device 102 and a cloud storage service

¹² The POR states that the '512 patent discusses "a secure backup of the records stored in the secure storage to a cloud storage service. ['512 patent] at 7:55-8:8." POR, p. 5. However, this is discussing elements at environment level of FIG. 1, which according to the PO's own expert does not illustrate the first and second processors. APPL-1031, p. 34 ("So figure 1 is just an illustration of the devices and the websites and cloud components. Instead, if you want to see an architecture diagram that shows a first processor and a second processor, an example would be figure 3.")

140. This communication path includes one or more intervening networks 110. As explained in the Petition, a cloud storage service was a known third party system providing a “geographically dispersed service[]” (Petition, pp. 60-61) that would include processors running on other devices. APPL-1030, ¶¶38, 40.

PO's reliance on the word “facilitate” used in other contexts does not save it. *See* POR, pp. 34-35. First, the word “facilitate” suggests making something easier, and Cheng's secure backup technique implemented in the context of a second (secure) processor in the Kesanupalli-Challener combination does far more than simply making secure backup easier. *See* Petition, pp. 54-57 (explaining, relative to limitation [1.7A], that Cheng 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-1030, ¶41. Moreover, PO does not construe “perform” to preclude involvement of downstream components along the path of the second processor's secure backup to a cloud storage service.

F. Additional claim arguments

1. Dependent Claims 2 and 12 are unpatentable over the Kesanupalli-Challener-Cheng combination

The POR arguments for these claims devolve to the same argument as set forth for the backup limitation, which fail for the reasons explained above. That argument ignores the actual position set forth in the Petition and accompanying declaratory evidence that a POSITA would have had reason and known how to

configure the second processor to perform the backup as discussed above and further, communication by the second processor that extends through the general processing area on the host PC is just what is described in the '512 patent. APPL-1030, ¶¶37-40, 42.

2. Independent Claims 11 and 21 are unpatentable over the Kesanupalli-Challener-Cheng combination

The POR provides no additional arguments for these claims, which are shown as obvious in the Petition. Petition, pp. 67-72.

II. CONCLUSION

For the reasons given in the Petition and accompanying declaratory evidence provided by Dr. McDaniel, as reinforced in this reply to PO's arguments in response, the Challenged Claims are obvious over the asserted prior art. PO does not rebut the legal or technological sufficiency of the evidence presented in this proceeding.

Respectfully submitted,

Dated: January 16, 2025
HAYNES AND BOONE PLLC
2801 N. Harwood Street, Suite 2300
Dallas, TX 75201

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

CERTIFICATE OF WORD COUNT

The undersigned attorney for Petitioner declares that the portions of this Reply subject to word count limitations of 37 C.F.R. §42.24(c)(1) have 5514 (less than 5,600) 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), service was made on Patent Owner as detailed below.

Date of service: January 16, 2025

Manner of service: Electronic Mail: Rkamprath@mckoolsmith.com;
gfishback@mckoolsmith.com;
Carbyne_Apple@mckoolsmith.com

Documents served: **Petitioner's Reply to POR;
EXHIBITS APPL-1030 – APPL-1035.**

Persons served: Richard A. Kamprath
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, Texas 75201

George Fishback
MCKOOL SMITH, P.C.
303 Colorado Street, Suite 2100
Austin, Texas 78701

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