

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC,
Petitioner,

v.

CARBYNE BIOMETRICS, LLC,
Patent Owner

IPR2023-00332
U.S. Patent No. 10,929,512

**SUPPLEMENTAL DECLARATION OF PATRICK MCDANIEL,
UNDER 37 C.F.R. § 1.68 IN SUPPORT OF PETITIONER’S REPLY**

TABLE OF CONTENTS

I.	Introduction.....	4
II.	Qualifications and Professional Experience.....	6
III.	Analysis	6
A.	Absence of Trusted Platform Module (TPM) or wiping description in Kesanupalli—the reference—would not be understood to indicate state of mind of Ramesh Kesanupalli—the person—or motivations of POSITA.....	7
B.	Kesanupalli is not only focused on preventing social engineering attacks; both wiping and use of a restricted interface are complementary to Kesanupalli’s teachings.....	10
C.	Dr. Goodrich’s suggestions regarding TPM adoption and deployment are errant and his conclusion that POSITA would exclude TPMs is incorrect and misleading	15
D.	Kesanupalli teaches secure storage and digitally-signed and authenticated binaries to protect credentials from malware; these device security teachings are complementary to, and do not obviate benefits of, TPM.....	18
E.	The <i>second processor</i> of Kesanupalli-Challener is configured to “perform a secure backup of the record to a storage service” when considered in combination with Cheng’s backup technique	23
F.	The ’512 patent provides for the backup of the record to include communication to the general processor (first processor)	24
G.	Secure backup of data on a user device to a storage service (cloud storage service) requires interim components	27
H.	Additional claim arguments	28
.1.	Dependent Claims 2 and 12 are unpatentable over the Kesanupalli-Challener-Cheng combination	28

.2.	Independent Claims 11 and 21 are unpatentable over the Kesanupalli-Challener-Cheng combination	28
IV.	Conclusion	29

I, Patrick McDaniel, do hereby declare as follows:

I. INTRODUCTION

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

2. I have been asked by Apple Inc. (“Apple”) to provide my expert opinion connection with the *Inter Partes* Review of U.S. Patent No. 10,929,512 (“’512 patent”) concerning whether the ’512 patent is unpatentable over certain prior art. This declaration is a statement of my opinions on a subset of issues relating to the patentability of Claims 1-6, 10-16 and 20-21 (“the Challenged Claims”) of the ’512 patent. More particularly, this declaration addresses certain conclusions drawn by Patent Owner’s Expert, Dr. Michael T. Goodrich, in his declaration (Ex. 2037) that I believe are vague or unclear, incorrect, unsupported or misleading. Should I not address a conclusion or statement, it does not imply that I agree Dr. Goodrich. As I explained more fully in my opening declaration (APPL-1003), and as I reaffirm now, it is my opinion that all the Challenged Claims would have been obvious to a person of ordinary skill in the art (“POSITA”) at the time of the alleged invention over the grounds detailed in that opening declaration.

3. I continue to be compensated for my work in this matter at my standard hourly rate. I am also being reimbursed for reasonable and customary

expenses associated with my work and testimony in this investigation. My compensation is not contingent on the outcome of this matter or the specifics of my testimony. I have no other financial interest in this proceeding.

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

Ex. 2037	Declaration of Dr. Michael T. Goodrich in Support of Patent Owner's Response for U.S. Patent No. 11,514,138
----------	---

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

- a) the documents listed above;
- b) my own knowledge and experience based upon my work in the field of authentication and distributed computing as described below, as well as the following materials including:

APPL-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
APPL-1034	Laptop Mag, Lenovo ThinkPad R500 Review, Jamie Bsales, August 20, 2008 (https://www.laptopmag.com/reviews/laptops/lenovo-thinkpad-r500), retrieved January 8, 2025
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
--	---

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

II. QUALIFICATIONS AND PROFESSIONAL EXPERIENCE

7. My Curriculum Vitae (CV) appears as APPL-1004. My Qualifications and Professional Experience remain substantially as described in my opening declaration (APPL-1003) and in my referenced CV (APPL-1004).

III. ANALYSIS

8. I have been asked to provide my opinion regarding certain conclusions drawn by Patent Owner's Expert, Dr. Michael T. Goodrich in his declaration (Ex. 2037). In doing so, I considered whether the alleged factual premise(s) for Dr. Goodrich's arguments were well-grounded or inaccurate and/or whether Dr. Goodrich's conclusions were supported or misleading. As described below, certain conclusions that Dr. Goodrich seeks to draw are incorrect, unsupported, misleading, or require additional context.

9. As indicated above, my opinions contained in this declaration are based on the documents I reviewed and my knowledge and professional judgment. My opinions have also been guided by my understanding of how a person of ordinary skill in the art would have understood the state of the art, the prior art, and

the claims and the specification of the '512 patent at the time of the alleged invention. I was informed that in the Institution Decision, the Board adopted Petitioner's POSITA standard except for the language "at least" that qualified the experience level stating it would allow the experience level to encompass an expert's level of skill. I apply the standard as clarified by the Board. The analysis of my declaration (APPL-1003) remains the same, applying this clarified level of skill for a POSITA.

A. Absence of Trusted Platform Module (TPM) or wiping description in Kesanupalli—the reference—would not be understood to indicate state of mind of Ramesh Kesanupalli—the person—or motivations of POSITA

10. I have also reviewed Dr. Goodrich's suggestion that Ramesh Kesanupalli—the person—made a "deliberate[] cho[ice] not to use a TPM" (trusted platform module) in Kesanupalli—U.S. Patent 8,799,666 (APPL-1006) — and Dr. Goodrich's conclusion that such a purported choice would have been indicative of the choice that a POSITA would make or otherwise persuasive on a POSITA. *See* Ex. 2037, p. 24 ("Ramesh Kesanupalli deliberately chose not to use a TPM"), ¶51 ("A POSITA would recognize this fact, and would not have been motivated to add the TPM architecture of Challenger.... Ramesh Kesanupalli (a POSITA) would not have been motivated to add a TPM to the Kesanupalli reference, which is further evidenced by the fact that Ramesh Kesanupalli in fact did not include a TPM in the Kesanupalli reference."), ¶64 (alleging that there are

“many reasons...why Ramesh Kesanupalli would consciously choose not to use TPMs in his patented system”).

11. First, a POSITA reviewing Kesanupalli reference would not conclude that the absence of a teaching (e.g., absence of wiping or TPM) is teaching an absence of that feature (e.g., wiping or TPM) in the system. Accepting such an assertion would imply that no modifications to any system were reasonable, and that any disclosure teaches away from any other approach or augmentation. This is simply not the perspective of a POSITA.

12. Second, I do not agree with Dr. Goodrich’s core premise that absence of reference to TPM or to a particular TPM standard, here ISO/IEC 11889-1:2009, in a patent application demonstrates a decision (conscious or otherwise) to reject a standards-based implementations of the techniques described or patented. Rather, as a patentee myself in heavily standardized fields of network and wireless communications, I find it far more likely that an inventor such as Ramesh Kesanupalli simply preferred that his disclosure be interpreted more broadly than with respect to a particular standard.

13. Third, and more specifically, I disagree with Dr. Goodrich’s suggestion that by omitting reference to a particular a TPM or naming the TPM standard, Ramesh Kesanupalli—the person—established himself as a surrogate for a POSITA’s decision regarding security enhancements. I recognized in my first

declaration for this matter the level of ordinary skill in the art. In my experience, a POSITA is not a lemming limiting themselves only to an explicit disclosure of a given patent but are instead motivated by perceived advantages of combining one prior art teaching with another. I reiterate as discussed in my first declaration, “[a] 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 CPU or microprocessor 30) the applications and other functions of Kesanupalli’s Host PC 202.” APPL-1003, ¶79. For example, I discussed a POSITA would have been motivated to apply Challenger’s teachings of a standards-based TPM architecture as an implementation framework for Kesanupalli’s biometric security techniques given the support a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided; 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 provide compatibility and robustness, and therefore engender trust amongst users and customers. APPL-1003, ¶¶83-84.

B. Kesanupalli is not only focused on preventing social engineering attacks; both wiping and use of a restricted interface are complementary to Kesanupalli's teachings

14. I have reviewed Dr. Goodrich's suggestion that U.S. Patent 8,799,666 to Kesanupalli reference "addresses social engineering attacks" and Dr. Goodrich's conclusion that, as such, Kesanupalli's teachings "aims are not furthered by TPMs, which provide device security." *See* Ex. 2037, ¶¶46, 51. I do not agree with either Dr. Goodrich's premise or his conclusion. Simply put, Kesanupalli's teachings are not constrained to *only* mitigating social engineering attacks. There is no requirement (explicit or implicit) in Kesanupalli that its authentication systems and methods only address social engineering attacks. 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.

15. While Kesanupalli facilitates the storage and use of secure, complex passwords by freeing a user from the difficult task of remembering those complex passwords—or worse remembering and typing a complex and unique password for each site and only for the right site, 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—which may highlight other risks, breach of the device providing access to the password

biometric information store(s). It addresses these risks of storing the sensitive information (breaches of the device) by providing security features. This is one reason why Kesanupalli describes numerous specific security features that are not focused exclusively on social engineering attacks or on promoting stronger passwords. Kesanupalli discloses numerous security features not constrained to a social engineering purpose. I detail several of these examples in the following paragraphs.

16. As one example, Kesanupalli is concerned with protection of user credentials (e.g., passwords and cryptographic keys) and biometric information in secure storage. For example, Kesanupalli describes that all user data is securely stored outside of the browser in a secure storage device: “The enrolled credentials of a user are encrypted with the encryption key and stored in a storage device. Such as secure storage 106. In a particular embodiment, biometric service 110 is implemented as a service application running in a local system account.” See APPL-1006, 6:6-10. Thereafter, the system of Kesanupalli uses that storage device in conjunction with a biometric sensor to support secure authentication, as an example, “An application 404 that desires to authenticate a user with a biometric device communicates with a biometric service 402, which is coupled to a secure storage.” APPL-1006, 7:2-4.

17. More broadly, Kesanupalli addresses numerous security features not

constrained to a social engineering purpose. 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-1006, 5:53-58, 6:15-17, 6:39-42. As one example, Kesanupalli discloses using secure socket layer (SSL) protocol for encrypted transmission of data including between its sensor and general processor. See APPL-1006, 1:28-30, 6:39-42. This addresses attacks in which the communication between process (programs) in an operating system can be compromised (addressing IPC eavesdropping attacks). Further, Kesanupalli discloses implementing strong cryptographic algorithms in its hardware and/or software which prevent compromise of data when stored (sometimes called offline or data-store attacks) or communicated between hosts and system components (eavesdropping attacks). See APPL-1006, 4:12-23. Further cryptography examples include using cryptography features of secure keys and hashes of the secure key, random challenge sensor ID, and the like. APPL-1006, 4:64-5:33 These methods further strengthen communication and storage security (again addressing offline and data-store attacks), as well as provide data freshness (preventing replay attacks). As another example, strengthening security by biometric sensor unique identifiers (ID), which makes bypassing biometric system authentication (often called masquerading attacks) very difficult. See APPL-1006, 4:23-30.

18. As yet another example, Kesanupalli uses digitally signed code and runtime checks for protection against man-in-the-browser attacks and malware. This prevents adversaries from replacing or corrupting the authentication service of Kesanupalli either before or during use. APPL-1006, 8:23-28. These protections are essential in modern systems to prevent attacks against the storage and runtime of running services.

19. I also note that the explicitly mentioned “dictionary attacks,” (Kesanupalli, APPL-1006, 1:35-38) are not social engineering attacks that trick or manipulate a user, but a different security risk mitigated by strong passwords. Dictionary attacks are not generally considered social engineering attacks, but are an attack that relies on automated attempts to guess a password through common words or phrases.

20. Any one of these features shows that Kesanupalli is concerned with security as a whole, including device security. This would also be the mindset of a POSITA approaching Kesanupalli as a POSITA would have reason and motivation to address security as a whole. In my opinion, Dr. Goodrich’s suggestion that Kesanupalli is focused solely on preventing social engineering attacks and his suggestions that Kesanupalli is not concerned with or directed to device security are each errant—indeed, such a perspective ignores the majority of security disclosures and discussion in the specification. Those suggestions are inconsistent

both with Kesanupalli's disclosure and with how that disclosure would be understood by a POSITA. Moreover, the conclusion that Dr. Goodrich draws from this errant suggestion is incorrect. Kesanupalli is most certainly directed to device-level protection in addition to social engineering attacks. As highlighted above, Kesanupalli provides defenses against an array of attacks using cryptographic, communications, storage and process level protections.

21. Further, I do not agree with Dr. Goodrich's distinction in applying Kesanupalli's teachings only attacks that are initiated by exploiting a social engineering security risk—tricking human users in a social engineering attack and breaching the actual device because attacks on a system are often interrelated. In my experience, social engineering attacks are often used as a precursor to other exploits or intrusions of the targeted device or its resources, services or data (e.g., to deploy malware).

22. Further, not only is Kesanupalli not focused solely on preventing social engineering attacks, a POSITA would not have approached a consideration of Kesanupalli with a mindset of addressing only type of attack. Security threats are multiple and multifaceted. This is the state of play in cyber-security at the time of the '512 patent; attackers will exploit any interface or asset they can access to accomplish their adversarial goal. Indeed, APPL-1032, which I understand to be a table of contents for a textbook by Dr. Goodrich, introduces as a fundamental

concept “Confidentiality, Integrity, and Availability,” which I understand to refer to the widely used CIA framework, which is a way of modeling (and therein addressing) the vast set of threats encountered by user programs like browsers. The CIA framework is illustrative of what would motivate a POSITA, a comprehensive security strategy that minimizes threats (of many origins) to each of the confidentiality, integrity, and availability of a system. That is, 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. Moreover, a 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.

C. Dr. Goodrich’s suggestions regarding TPM adoption and deployment are errant and his conclusion that POSITA would exclude TPMs is incorrect and misleading

23. I have also reviewed Dr. Goodrich’s suggestion that “practical considerations regarding TPM adoption and deployment in 2012 would motivate a POSITA to consciously exclude the use of a TPM with the Kesanupalli reference.” *See* Ex. 2037, ¶¶61-64, 40-43.

24. I do not agree with Dr. Goodrich’s premise(s) regarding adoption and

deployment. Well prior to 2012 (and December 2011), TPM was included on many enterprise-class PC and laptop motherboards deployments and the set of major PC manufacturers shipping TPM-enabled PCs include Dell, Lenovo, HP, Toshiba, and Fujitsu. Ex. 2042, p. 536. TPMs were widespread and ubiquitous and were well established as part of the toolchest available to POSITA for addressing security challenges.

25. Dr. Goodrich's appears to suggest that because "Microsoft [] announced that all systems submit[ed] to the Windows Certification Program after 1 January 2015 [would] be required to have TPM 2.0," that TPM adoption and deployment was not widespread until such time. *See* Ex. 2037, ¶42. That is incorrect. At least by 2009 Trusted Platform Modules (TPMs) were widely studied and deployed to enhance security for user applications. For example, Lenovo's T-series laptops, such as the ThinkPad T400 and T500, were notable for incorporating TPM chips. Lenovo's Windows XP SP2 TPM drivers on these laptops were used, for example, secure user authentication, encrypted file storage, and protection against unauthorized access. *See* APPL-1033, Lenovo ThinkPad T60p review.

26. Moreover, I do not agree with any suggestion that TPMs were not widespread and ubiquitous and/or would not have been well understood to a POSITA until their use was *required* as a baseline component for certifying

hardware for forthcoming versions of the Microsoft Windows® operating system. As a factual matter, TPMs were already widespread and ubiquitous. OEM PCs and laptops running the Microsoft Windows operating system had supported TPM. *See* Ex. 2042, p. 536; *see also*, APPL-1033 (2008 review of Lenovo ThinkPad T60p stating “[w]ith a view to security, there is a biometric fingerprint scanner on the main palm rest, which is linked to a Trusted Platform Module (TPM) chip”), APPL-1034 (2008 review of Lenovo ThinkPad R500 stating “the R500 includes a fingerprint reader and TPM circuitry to help keep data and corporate networks secure”); APPL-1035 (Lenovo PC support website listing Intel integrated TPM drivers with “09 Jun 2009” release dates for various Lenovo laptops running Windows XP Service Pack 2). ThinkPad laptops such as the forgoing with on-board TPM that interfaced with integrated fingerprint readers were familiar to me personally well before 2012.

27. Furthermore, in my experience, uplifts to the Microsoft Windows baseline of *required* hardware occur many years after an underlying technique or component (here a TPM chip) has been widely deployed in OEM equipment and the newly required hardware is well understood. As a practical matter, any technology must have been (and was in the case of TPMs) vetted and proven to be stable, useful and secure over many years before a company like Microsoft would require it on literally billions of computers worldwide. Here, the announcement by

Microsoft relied upon by Dr. Goodrich—a 2013 announcement with effect beginning in 2015—that TPM would be required future Windows operating system compatibility is entirely consistent with the widespread and ubiquitous nature of TPM that I demonstrate above.

D. Kesanupalli teaches secure storage and digitally-signed and authenticated binaries to protect credentials from malware; these device security teachings are complementary to, and do not obviate benefits of, TPM

28. Finally, I have reviewed Dr. Goodrich’s assertion that “the Kesanupalli reference discloses a system that already provides an end-to-end secure system” and his conclusion that “POSITA would understand [that such a secure system] would not be made more secure with the addition of a TPM.” *See* Ex. 2037, ¶¶56-60.

29. Kesanupalli teaches device security in the form of secure storage for credentials and biometric information. The included protections provide for secure operation of programs like browsers, even in the presence of things like “Man in the browser” attacks. APPL-1006, 3:14-4:11. Kesanupalli also teaches the use of digitally-signed binaries (executable code) as well as authentication and runtime validation of such binaries to limit malware risks. Such protections prevent malicious code on the operating system from compromising the authentication service itself and allowing users to be masquerading or exfiltrating user credentials. APPL-1006, 8:23-28; *see also* Ex. 2037, ¶59 (citing same). These

teachings are of device protection and device-side security to limit access to sensitive data and reduce malware risk.

30. Accordingly, I do not disagree that Kesanupalli’s teachings extend well beyond mitigation of social engineering attacks to these end-to-end techniques at the device. However, Dr. Goodrich’s assertion that “POSITA would understand [Kesanupalli teaches a system that] would not be made more secure with the addition of a TPM” (Ex. 2037, ¶56), that “POSITA would not be motivated to add a TPM to the Kesanupalli reference” (Ex. 2037, ¶57), or that “adding a TPM to the Kesanupalli reference’s system would not result in security benefits” (Ex. 2037, ¶60) are incorrect.

31. First, the augmentation of Kesanupalli with a TPM follows the best practices of “defense in depth.” Defense in depth is a security strategy that uses multiple independent layers of security apparatus to protect systems or programs at risk. This approach ensures that if one layer is breached, additional layers remain to counteract the threat, creating a more resilient overall defense. By multiple techniques, defense in depth minimizes vulnerabilities and increases the difficulty for attackers to compromise sensitive assets. This layered strategy acknowledges the complexity of modern threats and the need for a multifaceted response to secure systems comprehensively.

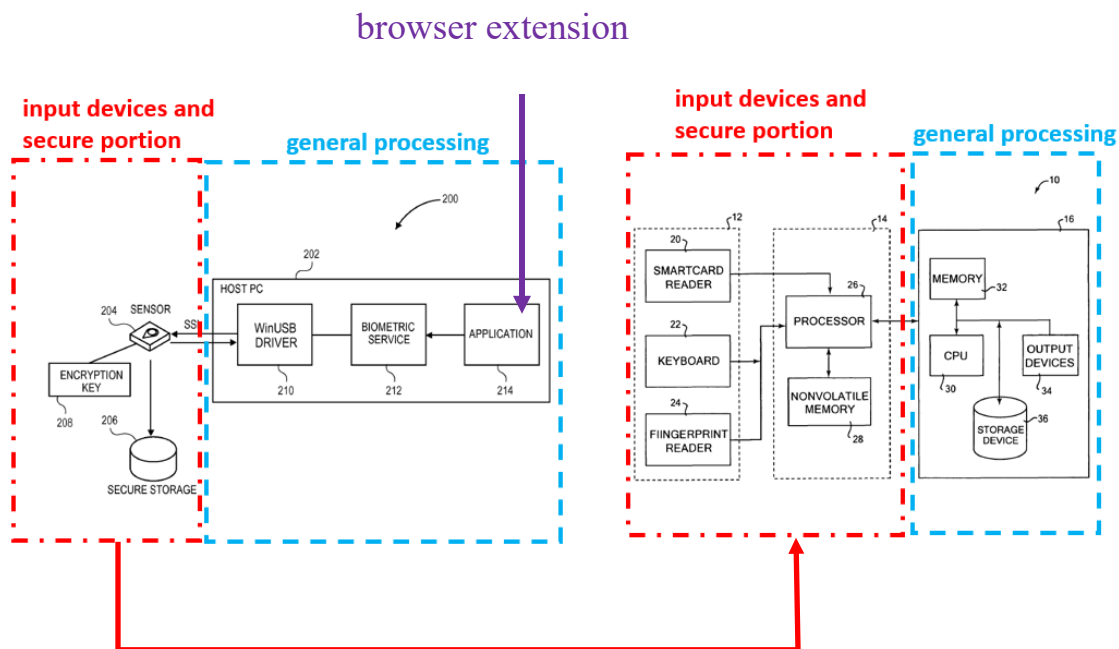
32. Adding TPMs to security-sensitive services like authentication

strengthens the system against several classes of attacks. For example (and to name only a few), TPMs prevent keylogging attacks by securely generating and storing cryptographic keys within the hardware, making them inaccessible to malware. They also mitigate man-in-the-middle (MITM) attacks by enabling secure, hardware-based authentication protocols that verify both the user and the system. Additionally, TPMs resist offline attacks, such as brute force attempts to guess credentials, by requiring physical access to the device for key operations. By anchoring security in hardware, TPMs create a robust barrier that complements other security mechanisms.

33. The combination of Kesanupalli's system with a TPM-based architecture would realize the benefits of defense in depth. Kesanupalli's authentication service would gain additional strength from TPM's hardware-level protections, effectively addressing vulnerabilities across multiple attack vectors. This integration would establish a layered security framework that ensures that even if one security mechanism is bypassed or compromised, the system remains protected.

34. Additionally, I discussed in my earlier declaration, a POSITA deploying the security functions of Kesanupalli's would have been motivated to implement those functions on Challenger's TPM-based security architecture using specialized security processor, including its restricted interfaces, such as illustrated

by Challenger's security processor 26. Whether Kesanupalli digitally signs or checks binary files for validity prior to running them in its browser extension of its **general processor** is an entirely different security feature than provided by Challenger's teachings directed to its **security processor** and interfaces thereto. A POSITA however clearly understands that security is multi-faceted and provided throughout a system's architecture. And thus, addresses security in different ways and at different portions of the system.



35. I understand Dr. Goodrich to state that “[i]n 2012, compatibility issues with existing systems and software could be caused by implementing TPMs. This is because mainstream systems and software did not support TPMs.” Ex. 2037, ¶62. I understand Dr. Goodrich to base his issue of compatibility with a lack of

adoption, which as I discuss above is incorrect. I know of no compatibility issues, nor do I find any compatibility issues identified in Dr. Goodrich's declaration that would preclude a POSITA from having a reasonable expectation of success in applying Challenger's TPM-based architecture and API-mediated interfaces to Kesanupalli's authentication technique. As I discussed in my first declaration and as illustrated by the Figures reproduced above, Challenger and Kesanupalli share a similar configuration.

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

36. Dr. Goodrich concludes, without description as to *why*, that it would have been very difficult to implement a technique “where a TPM backed up its records to any storage service[,]” while protecting the data. Ex. 2037, ¶65. See also, Ex. 2037, ¶71, “[c]reating a system that would address these issues [or backup of the data in the TPM] would be a monumental task absent the teachings of the ’512 Patent itself.” Ex. 2037, ¶71. I disagree. I described in my original declaration that backing up signing data and keys of a TPM (such as the records in secure storage) was well known and widely deployed (APPL-1003, ¶¶159-160), that the implementation would protect the process of securely backing up biometric data and user credentials from a myriad of potential attacks (APPL-1003, ¶161), and the process of porting code from OS-native to TPMs was well understood and widely practiced by the priority date including that the APIs and code structures for such a port were well documented at the time (APPL-1003, ¶162). Cheng’s backup process provides encryption protection of the data. APPL-1008, FIGS. 3A-3B, [0023]–[0029]. Implementing a technique where a TPM backed up its records to any storage service while protecting the data would have been predictable and easy to implement by a POSITA. In fact, Cheng states an onboard microprocessor of the biometric-based authentication device performs the backup. APPL-1008, [0022]. A

POSITA would recognize that this means a processor similarly included in a biometric-based authentication device such as the secure process of Kesanupalli-Challener is suitable for configuration to perform a secure backup. The secure processor (*second processor*) of the Challener architecture implementing Kesanupalli's techniques has access to the records in secured storage and capability to perform the encryption desired in Cheng. (Challener) APPL-1007, FIG. 1, 4:24-36; (Kesanupalli) APPL-1006, 6:42-45. I discussed this in my first declaration including at APPL-1003, ¶173.

F. The '512 patent provides for the backup of the record to include communication to the general processor (first processor)

37. First, a TPM being restricted or preventing unauthorized access does not mean there is no interaction with the outside world. A POSITA would understand that code running within the TPM would be able to exchange messages and/or data with general processor resources, albeit in a controlled manner. See my discussion in APPL-1003 including ¶¶160-163 including my citation to Infineon TPM Key Backup and Recovery for Trusted Platforms, APPL-1018, p. 3 (describing secure backup protocol elements created by TCG standardization group and implemented by Infineon Professional Package for its TPM implementation).

38. Performing a secure backup to a storage service such as a cloud storage service necessarily includes other components, including other processors outside of the *second processor*. Fig. 1 of the '512 patent is illustrative of the

communication path between a user device 102 and a cloud storage service 140.

This communication path includes one or more intervening networks 110. I

explained in my first declaration, a cloud storage service was a known third party system providing a geographically dispersed service that would include processors

running on other devices. A POSITA would understand that numerous

intermediate devices would exist along the path between user device 102 and a

cloud storage service 140, including servers, routers, storage controllers and the

like operating to communicate effectuate secure communication of backup data to

a repository that would typically be distant, and indeed, geographically separated,

from the user device 102.

39. Third, 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. 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. 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 fast processor (*first processor*). 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.”). From the insecure storage, a POSITA would understand that the fast processor (*first processor*) would be involved in transmitting the encrypted and MACed backup data in the manner described above in paragraph 38, e.g., via numerous intermediate devices would exist along the path between user device 102 and a cloud storage service 140. Thus, Dr. Goodrich’s attempt to characterize the secure processor (*second processor*) as performing the secure backup without any communication with the first processor is in conflict with the '512 patent’s disclosure.¹

¹ The '512 patent at 7:55-8:8 discussing elements at environment level of FIG. 1, which does not illustrate the first and second processors.

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

40. Dr. Goodrich appears to argue that the claim requires the second processor have an exclusive role in performing the backup to the storage service. See, e.g., Ex. 2027, ¶69 (“is not met if the first processor performs or completes the performance of a secure backup of the record to a storage service”). A POSITA would not understand any requirement for the *second processor* have an exclusive role in the *secure backup...to a storage service*. Performing a secure backup to a storage service such as a cloud storage service necessarily includes other components, including other processors outside of the secure processor (*second processor*). As I discuss above, Fig. 1 of the ’512 patent is illustrative of the communication path between a user device 102 and a cloud storage service 140. This communication path includes one or more intervening networks 110. A cloud storage service was a known third party system providing a geographically dispersed service that would include processors running on other devices.

41. A POSITA would understand the word “facilitate” suggests making something easier. 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. 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)). A

POSITA would not understand the term “perform” to preclude involvement of downstream components along the path of the second processor’s secure backup to a cloud storage service.

H. Additional claim arguments

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

42. Dr. Goodrich states that “Kesanupalli reference’s sensor with the Challener reference’s TPM only connects to the Host PC through an SSL connection” and “TPM cannot ‘perform a secure backup of the record to a storage service.’” Ex. 2037, ¶73. This argument is the same argument as set forth for the backup. As I explained in my declaration (EX1003) and above, 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.

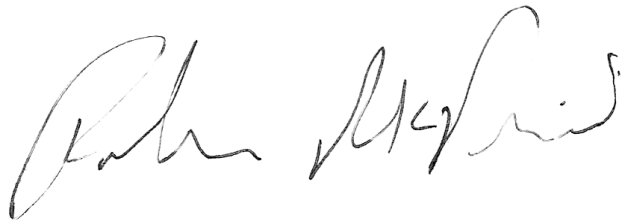
.2. Independent Claims 11 and 21 are unpatentable over the Kesanupalli-Challener-Cheng combination

43. Dr. Goodrich provides no additional arguments for these claims. Ex. 2037, ¶74.

IV. CONCLUSION

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

Date: January 16, 2025

A handwritten signature in black ink, appearing to read "Robert McDaniel", is written over the signature line.