

Inter Partes Review

U.S. Patent No. 11,514,138

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

[Apple Inc. v. Carbyne Biometrics., Case IPR2024-00334](#)

[Apple Inc. v. Carbyne Biometrics., Case IPR2024-00332](#)

David O'Brien, Haynes and Boone, LLP

Kelly Lyle, Haynes and Boone, LLP

Hong Shi, Haynes and Boone, LLP

'138 Patent Claims Challenged

F. The Asserted Grounds of Unpatentability

Petitioner asserts that the challenged claims of the '138 patent are unpatentable based on the following grounds (Pet. 11, 54, 62, 70):

Claims Challenged	35 U.S.C. §	References/Basis
1–3, 7, 8, 12–15, 19, 24, 25	103(a) ⁸	Kesanupalli, Brown
10, 22	103(a)	Kesanupalli, Brown, Cheng
11, 23	103(a)	Kesanupalli, Brown, Challenger
5, 17	103(a)	Kesanupalli, Brown, Headley

(IPR2024-00334) Inst. Dec. (Paper 10), 10.

'512 Patent Claims Challenged

E. Prior Art and Asserted Grounds

Petitioner asserts that claims 1–6, 10–16, 20, and 21 would have been unpatentable on the following ground (Pet. 9):

Claim(s) Challenged	35 U.S.C. §	References/Basis
1–6, 10–16, 20, and 21	103(a) ¹	Kesanupalli, ² Challener, ³ Cheng ⁴

(IPR2024-00332) Inst. Dec. (Paper 10), 10.

Claim 1, '138 Patent

1. A device, comprising:
a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
a biometric template; and
a credential comprising a cryptographic key;
in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
establish a connection with the external resource;
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.

Claim 1, '512 Patent

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

('512 Patent, claim 1) APPL-1001, 10:62-11:31.

Summary Claim Landscape

General Claim Terms	'138 Patent IPR2024-00334	'512 Patent IPR2024-00332
processor	✓	
first processor / second processor		✓
record (biometric template and/or credential (key))	✓	✓
match (biometric input and biometric template)	✓	✓
facilitate login to external resource (transmit credential)	✓	✓
wiping of record	✓	
secure backup of record	✓ (dependent)	✓
restricted interface	✓ (dependent)	✓

Discussion Roadmap

- '138 Patent Grounds:

- **Prior Art Teachings Not Seriously Disputed** **Slides 7-14**
- Motivation to Combine Kesanupalli and Brown **Slides 21-33**
- Motivation to Combine Kesanupalli-Brown and Challenger **Slides 21-37**

- '512 Patent Grounds:

- **Prior Art Teachings Not Seriously Disputed** **Slides 15-19**
- Motivation to Combine Kesanupalli-Cheng and Challenger **Slides 21-37**
- Petition demonstrates “*a second processor is configured to: ... perform a secure backup of the record to a storage service*” **Slides 39-49**

'138 Patent

Prior Art Teachings Not Seriously Disputed

Undisputed: Kesanupalli Teaches Limitations [1.1]-[1.7], [1.9] of '138 Patent, Claim 1

1. A device, comprising:

a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:

based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;

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

a biometric template; and

a credential comprising a cryptographic key;

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

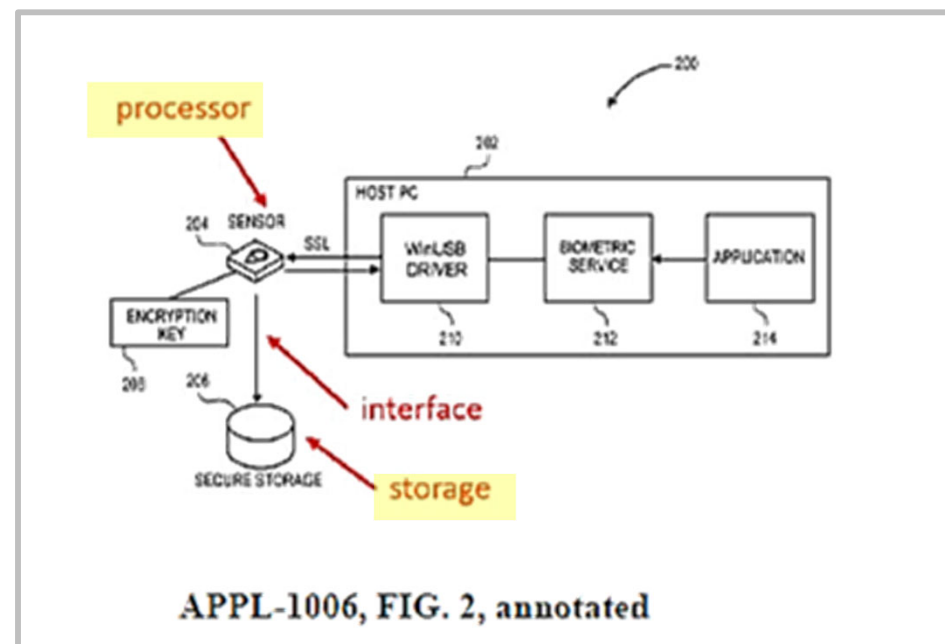
establish a connection with the external resource;

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

facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and

a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.



(Kesanupalli) APPL-1006, Fig. 2, annotated;
(IPR2024-00334) Pet., 24;
(IPR2024-00334) APPL-1003, ¶194.

Kesanupalli's system includes a main memory, a *memory*. APPL-1006, 9:58-10:46 ("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 *processor* and configured to provide the processor with *instructions* including at least those that execute the functions of Host PC 202. APPL-1003, ¶151.

(IPR2024-00334) Pet. (Paper 2), 44.

Undisputed: Kesanupalli Teaches Limitations [1.1]-[1.7], [1.9] of '138 Patent, Claim 1

1. A device, comprising:
a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
a biometric template; and
a credential comprising a cryptographic key;
in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
establish a connection with the external resource;
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.

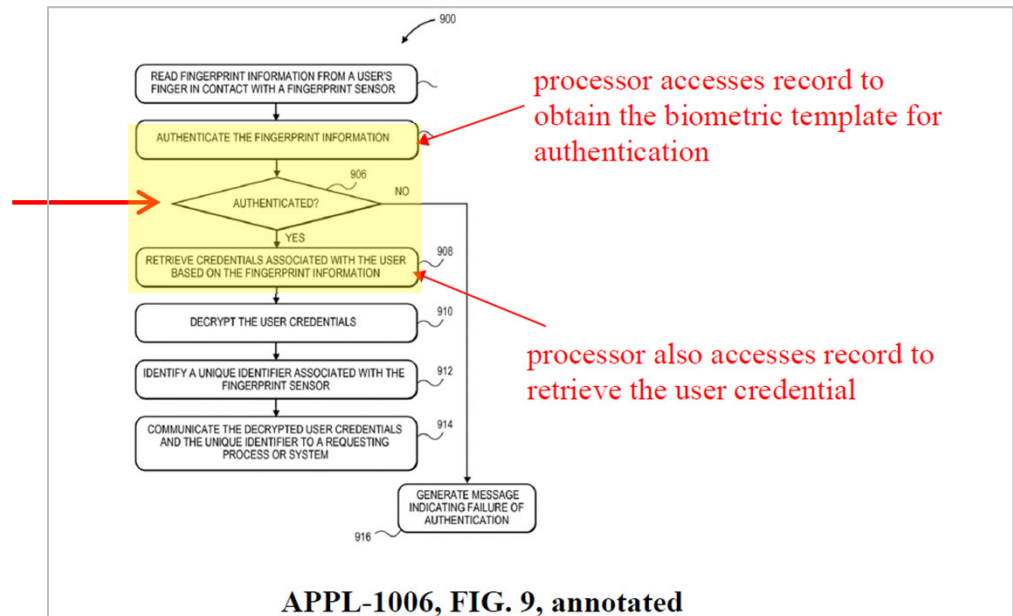
With respect to limitation [1.3], Kesanupalli describes a user's enrollment process for an external resource such as a website where the user's credential and biometric template are stored in secure storage. APPL-1006, 3:15-51 ("Initially, a user enrolls with the biometric user authentication system 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.")

(IPR2024-00334) Pet., 26; (Kesanupalli) APPL-1006, 3:15-51.

Undisputed: Kesanupalli Teaches Limitations [1.1]-[1.7], [1.9] of '138 Patent, Claim 1

1. A device, comprising:
 a processor on the device;
 a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
 based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
 wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
 a biometric template; and
 a credential comprising a cryptographic key;
 in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voice-print, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
 establish a connection with the external resource;
 facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
 facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
 a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.



(Kesanupalli) APPL-1006, FIG. 9, annotated;
 (IPR2024-00334) Pet. (Paper 2), 26; (IPR2024-00334) APPL-1003, ¶106.

Kesanupalli's authentication process includes determining a match between a biometric input (e.g., fingerprint information) and the biometric template (e.g., fingerprint template) and if there is a match, in response retriev[ing], from the at least one record, the credential. APPL-1006, 9:14-20 ("The procedure then **authenticates the fingerprint information** (block 904)...If the fingerprint information is authenticated, the procedure **retrieves credentials** associated with the user based on the fingerprint information (block 908)."), 6:31-49 ("For example, in a successful fingerprint swipe, the swiped fingerprint information matches a fingerprint template associated with the fingerprint sensor...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..."), 3:52-56 ("During an example user identification process

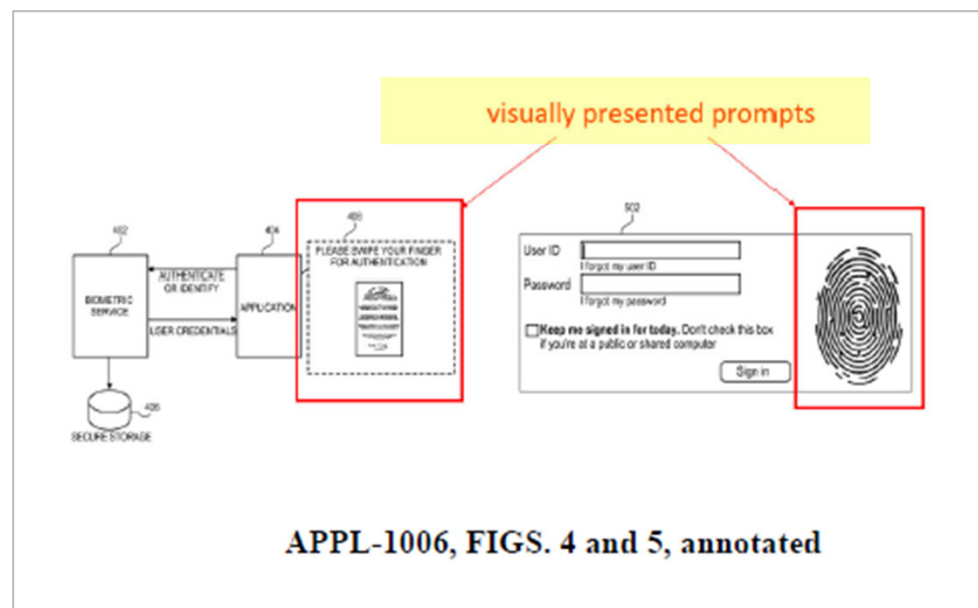
(Kesanupalli) APPL-1006, 6:31-49;

(IPR2024-00334) Pet. (Paper 2), 31-32; (IPR2024-00334) APPL-1003, ¶119.

Undisputed: Kesanupalli Teaches Limitations [1.1]-[1.7], [1.9] of '138 Patent, Claim 1

1. A device, comprising:
a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
a biometric template; and
a credential comprising a cryptographic key;
in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
establish a connection with the external resource;
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.

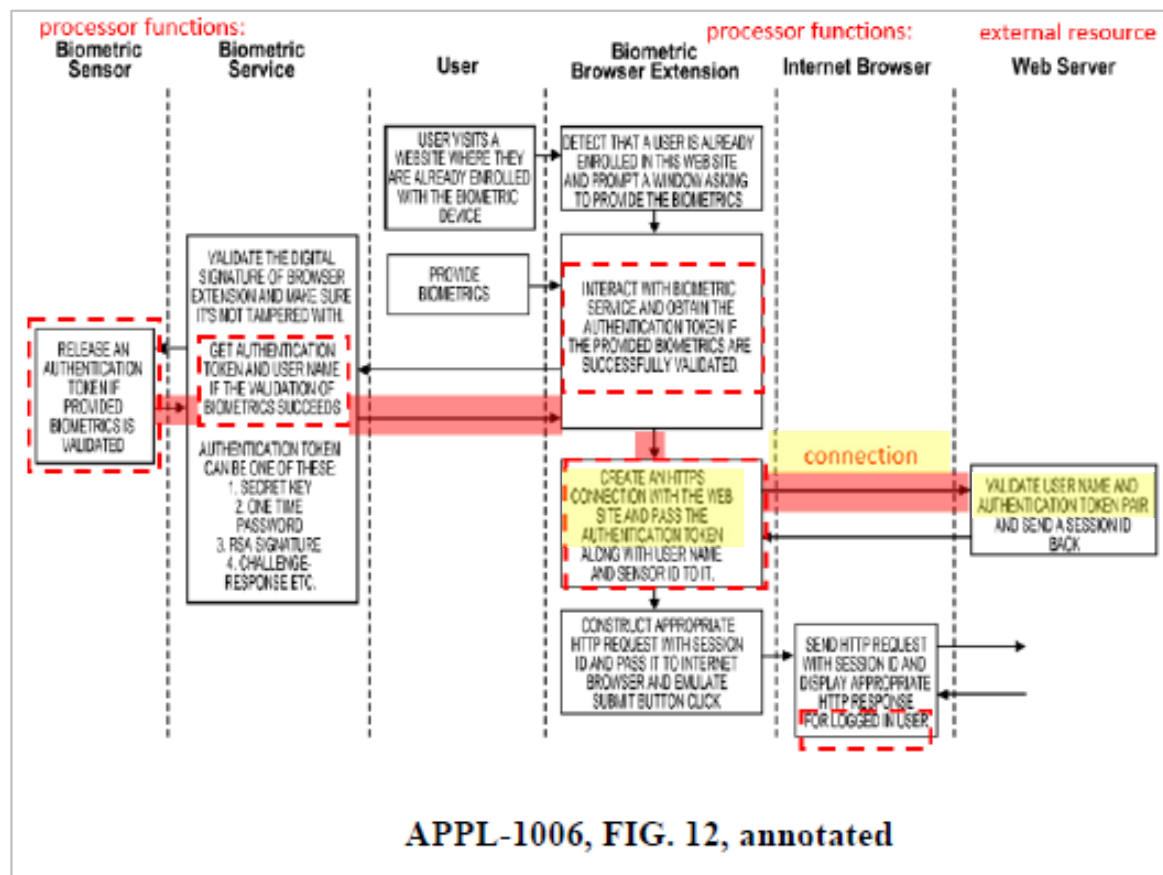


(Kesanupalli) APPL-1006, FIGS. 4-5, annotated;
(IPR2024-00334) Pet. (Paper 2), 34-35; (IPR2024-00334) APPL-1003, ¶126.

Undisputed: Kesanupalli Teaches Limitations [1.1]-[1.7], [1.9] of '138 Patent, Claim 1

1. A device, comprising:
a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
a biometric template; and
a credential comprising a cryptographic key;
in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
establish a connection with the external resource;
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
a memory coupled to the processor and configured to provide the processor with instructions.

('138 Patent, claim 1) APPL-1001, 11:17-56.



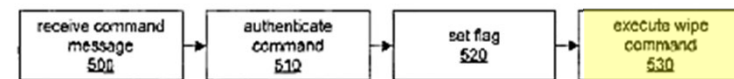
(Kesanupalli) APPL-1006, FIG. 12, annotated;
(IPR2024-00334) Pet. (Paper 2), 39; (IPR2024-00334) APPL-1003, ¶135.

Undisputed: Brown Teaches Limitation [1.8] – “wiping”

1. A device, comprising:
a processor on the device;
a storage on the device that is accessible by the processor on the device via an interface that facilitates communication between the storage on the device and the processor on the device, wherein the processor on the device is configured to:
based at least in part on a request from a user to access an external resource, facilitate, using the interface, access of at least one record stored at least in part in the storage on the device;
wherein the at least one record is associated at least with the external resource, and wherein the at least one record comprises:
a biometric template; and
a credential comprising a cryptographic key;
in response to determining a match between a biometric input and the biometric template, retrieve, from the at least one record, the credential, wherein the biometric input corresponds to at least one of a fingerprint, a feature usable for facial recognition, a voiceprint, a feature usable for a retina scan, or a typing feature, wherein the biometric input is received subsequent to presenting of a prompt, wherein the prompt comprises a prompt to provide biometric information, and wherein the prompt is visually presented;
establish a connection with the external resource;
facilitate a login of the user to the external resource at least in part by transmitting, via the established connection, output based at least in part on the credential retrieved from the at least one record, and wherein the user is logged in to the external resource based at least in part on the output; and
facilitate wiping of both the biometric template and the credential comprising the cryptographic key of the at least one record stored at least in part in the storage on the device; and
a memory coupled to the processor and configured to provide the processor with instructions.

(’138 Patent, claim 1) APPL-1001, 11:17-56.

Brown discloses a system and method for deleting or wiping data, including personal data, from a user’s electronic device. APPL-1003, ¶¶143-145; APPL-1009, Abstract. *See also*, APPL-1009, 1:15-18, 2:7-15, 11:65-13:14 (describing the method of FIG. 6). FIG. 6 of Brown is illustrative of executing its wipe command at a user’s device such as a personal computer, mobile device or the like:



APPL-1009, FIG. 6

APPL-1009, 4:64-5:11, 11:65-66 (FIG. 6 is a flowchart of “execution of the wipe command on the client device[.]”). Brown describes that it may be desirable to

(IPR2024-00334) Pet. (Paper 2), 41; (IPR2024-00334) APPL-1003, ¶143.

Undisputed: Challenger Teaches
Claims 11, 23 – “restricted interface”

'138 Patent, Ground 3 :

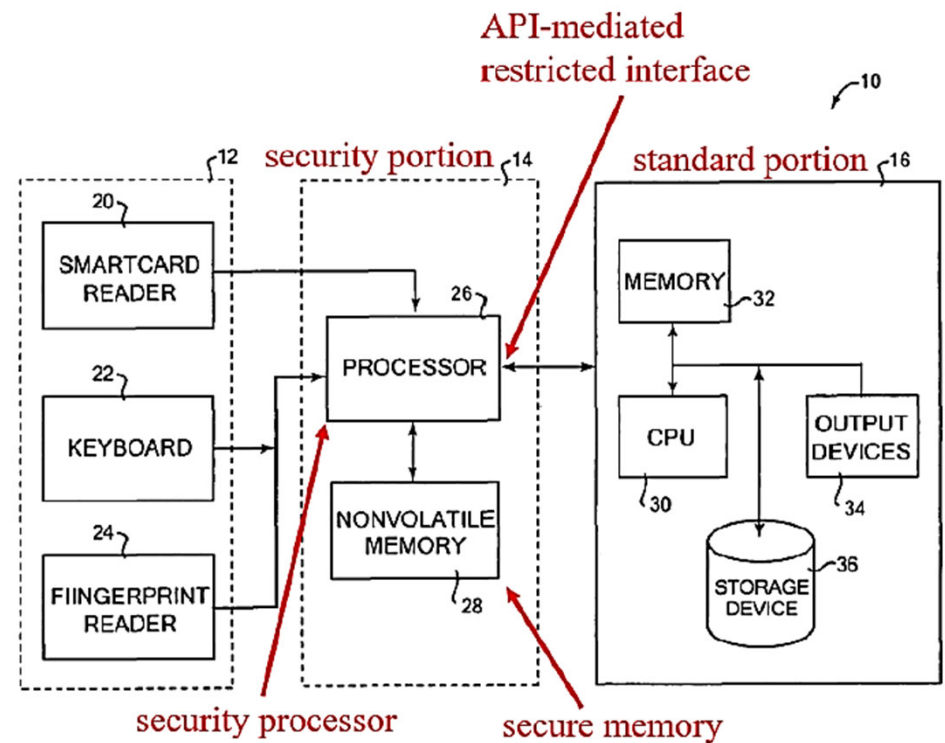
11. The device recited in claim 1, wherein the interface comprises a restricted interface.

('138 Patent) APPL-1001, 12:16-17.

23. The method of claim 13, wherein the interface comprises a **restricted interface**.

('138 Patent) APPL-1001, 13:13-14.

POSITA would have been motivated to implement the functionality of sensor 204 of Kesanupalli using Challener's teachings of providing secure processor functions (26) and Kesanupalli's secure memory 206 using Challener's corresponding secure memory, non-volatile memory 28. *See supra* Section IX.C.2.; APPL-1003, ¶¶200-202, 204-205; APPL-1007, 4:57-65 ("memory 28 is a secure memory which cannot be easily tampered with to read its data contents. In



APPL-1007, FIG. 1, annotated

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

(IPR2024-00334) Pet. (Paper 2), 63, 67; (IPR2024-00334) APPL-1003, ¶¶195-211.

'512 Patent

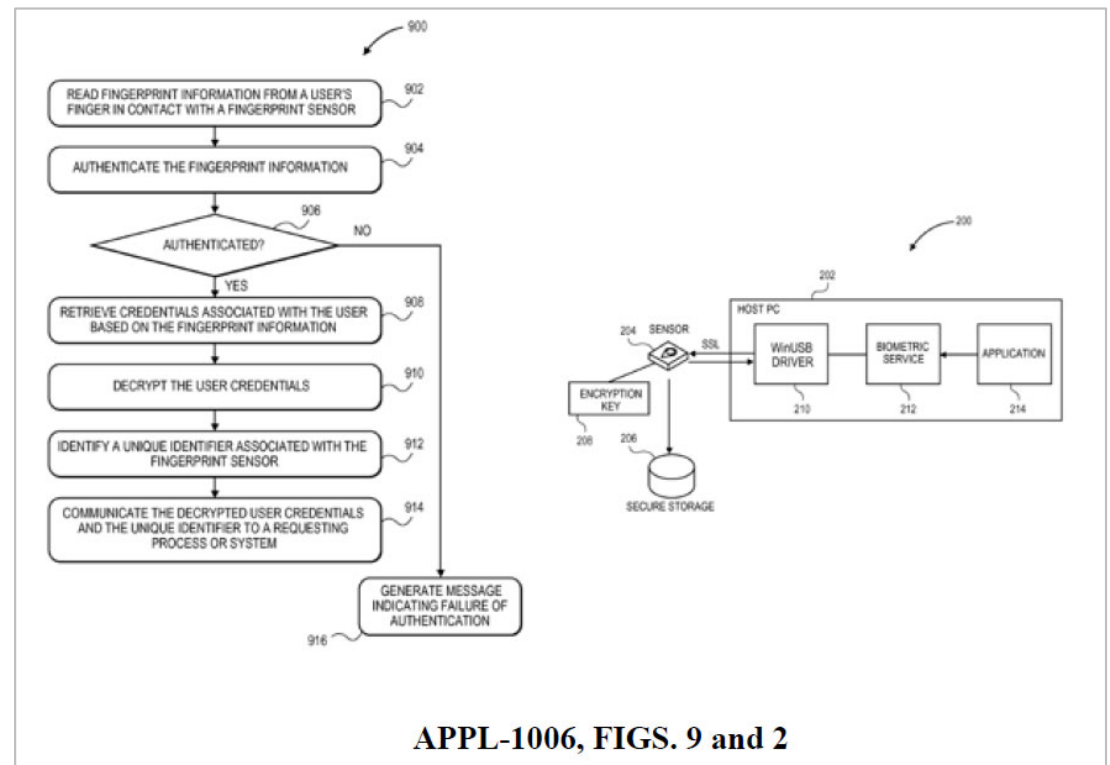
Prior Art Teachings Not Seriously Disputed

Undisputed: Kesanupalli Teaches Authentication Limitations of '512 Patent, Claim 1

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

('512 Patent, claim 1) APPL-1001, 10:62-11:31.

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

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

(IPR2024-00332) Pet. (Paper 2), 11-12; (IPR2024-00332) APPL-1003, ¶165.

Undisputed: Cheng Teaches *Secure Backup*

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

(‘512 Patent, claim 1) APPL-1001, 10:62-11:31.

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

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.”)

(IPR2024-00332) Pet. (Paper 2), 54-56; (IPR2024-00332) APPL-1003, ¶¶158-165.

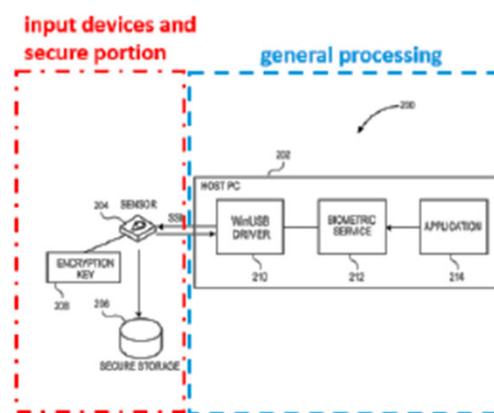
Undisputed: Challenger Teaches a System Implementation having a *First* and *Second* Processor

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

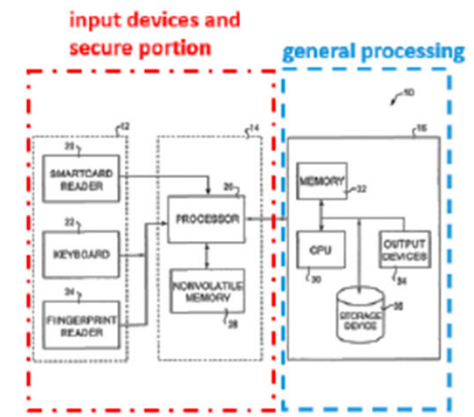
(‘512 Patent, claim 1) APPL-1001, 10:62-11:31.

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;

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)



Kesanupalli, FIG. 2, Annotated



Challenger, FIG. 1, Annotated

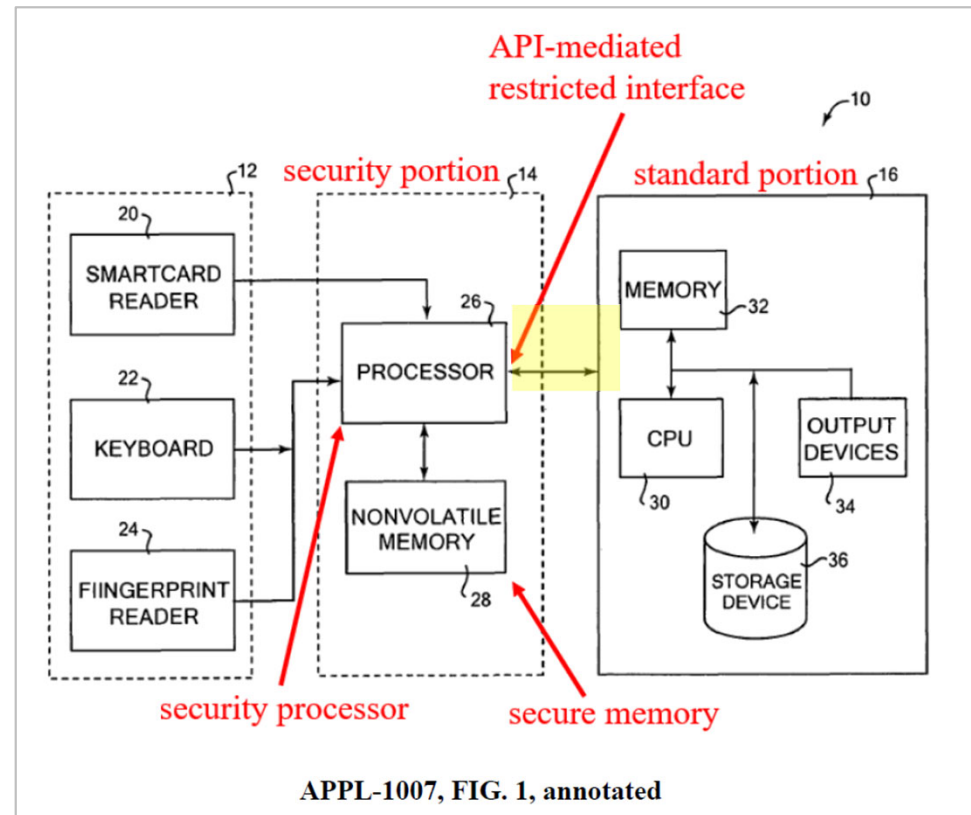
Undisputed: Challenger Teaches a System Implementation having a *Restricted Interface*

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a **restricted interface**, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

('512 Patent, claim 1) APPL-1001, 10:62-11:31.

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



Discussion Roadmap

- '138 Patent Grounds:

- Prior Art Teachings Not Seriously Disputed Slides 7-14
- Motivation to Combine Kesanupalli and Brown Slides 21-33
- Motivation to Combine Kesanupalli-Brown and Challenger Slides 21-37

- '512 Patent Grounds:

- Prior Art Teachings Not Seriously Disputed Slides 15-19
- Motivation to Combine Kesanupalli-Cheng and Challenger Slides 21-37
- Petition demonstrates “*a second processor is configured to: ... perform a secure backup of the record to a storage service*” Slides 39-49

Petition Established Motivation to Combine for Each Challenge

Obvious to a POSITA (pre-AIA) 35 U.S.C. §103(a):

'138 Patent (IPR2024-00334)	
Kesanupalli + Brown	✓
Kesanupalli + Brown + Cheng	✓
Kesanupalli + Brown + Challenger	✓
Kesanupalli + Brown + Headley	✓
'512 Patent (IPR2024-00332)	
Kesanupalli + Cheng + Challenger	✓

Patent Owner purports to raise reasons to not combine

These arguments fail as they demand an overly narrow perspective for the obviousness inquiry:

Mr. Kesanupalli's selection of features
for inclusion in his patent application

Kesanupalli's recognition of social
engineering attacks being a threat

Petition's Reasons to Combine Brown with Kesanupalli Are Not Seriously Disputed ('138 Patent)

	“need or problem known in the field” <i>KSR</i>, 127 S.Ct. at 1742	Pet., 18 (“POSITA would have readily understood the stored biometric information and credentials would be <u>at risk</u> if Kesanupalli’s device were <u>lost or stolen</u>”); Pet. Reply, 2.
	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 18-19 (“Brown’s system and method for wiping data at a communication device including according to a predefined rule would provide <u>an advantage for client devices</u> like those of Kesanupalli—namely, that of <u>protecting data on the client device from unauthorized use</u> by wiping it from the device”); Pet. Reply, 13.
	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 19 (“adding <u>a wiping technique</u> of Brown in <u>a biometric authentication system</u> such as taught by Kesanupalli as Brown is similarly directed to improving security of personal information in a substantially similar device. ... the wiping technique of Brown is implemented by routine software executed on generic processing components, which would have been a predictable application relative to Kesanupalli’s system and devices. APPL-1003, ¶81. Brown discloses that <u>a processor facilitates its wiping techniques.</u>”)

(IPR2024-00334) Pet. (Paper 2), 18-19;

(IPR2024-00334) APPL-1003, ¶¶75-82.

(IPR2024-00334) Pet. Reply (Paper 16), 2-14; APPL-1036, ¶¶10-23.

Petition's Reasons Combine Challenger with Kesanupalli-Brown Are Not Seriously Disputed ('138 Patent)

✓	“need or problem known in the field” <i>KSR</i> , 127 S.Ct. at 1742	Pet., 62 (“Challenger, in accord with the <u>TPM specification</u> , a standard chipset including a programmable microcontroller can be provided and used to store and secure information of the <u>system that is desired to be protected</u> ”)
✓	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 65-66 (“standards-based architecture as an implementation framework for Kesanupalli’s biometric security techniques given the support that a TPM implementation provides for many of the underlying cryptographic security services (encryption/decryption) and secure storage facilities provided...These are precisely the security architecture features POSITA having Kesanupalli before them would be motivated to implement in a <u>standards-based security architecture</u> that would engender trust amongst users and customers.”)
✓	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 66 (“implementing Kesanupalli’s biometric authentication techniques and in applying Brown’s wipe features to a sensitive data in secure storage given that Challenger’s architecture applies <u>TPM techniques, which were well-known, standard and widely-deployed in the industry.</u> ”); Reply, 18-19; APPL-1036, ¶25 (“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.”)

(IPR2024-00334) Pet. (Paper 2), 62-66;
 (IPR2024-00334) APPL-1003, ¶¶51-54 (TPM), 195-197 (Challenger), 198-202 (Combination);
 (IPR2024-00334) Pet. Reply (Paper 16), 14-20; APPL-1036, ¶¶24-36.

Petition's Reasons to Combine Challenger with Kesanupalli-Cheng Are Not Seriously Disputed ('512 Patent)

	“need or problem known in the field” <i>KSR</i>, 127 S.Ct. at 1742	Pet., 13 (“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 <u>desired to be protected</u>. APPL-1003, ¶¶67-69, 45-51.”); Pet. Reply, 14-15.
	“obvious benefit” and “predictable results” <i>Id.</i> at 1731, 1739, 1740, 1744	Pet., 19-20 (“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 <u>proven, widely adopted security architecture</u> and who would expect that the <u>marketplace would favor a standards-based implementation</u>. APPL-1003, ¶¶78.”); Pet., 24 (“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 <u>engender trust amongst users and customers</u>. APPL-1003, ¶¶83, 48-51; APPL-1016; APPL-1017 (describing TPM adoption).”); Pet. Reply, 11-12.
	“a combination of familiar elements according to known methods” <i>Id.</i> at 1739	Pet., 19 (“A well-known platform for implementing secure systems and for securely handling sensitive information is <u>a Trusted Platform Module (TPM) security architecture</u>. APPL-1003, ¶¶77, 45-51. TPM implementations were <u>widely implemented based on specifications from Trusted Computing Group (TCG)</u> and would have been well understood by POSITA before the earliest priority date of the '512 patent. <i>Id.</i>”); Pet., 24 (“implementing Kesanupalli’s biometric authentication techniques in Challenger’s TPM-based architecture, as <u>TPMs were well-known, standard and widely-deployed in the industry</u>.”); Reply, 14-15; APPL-1030, ¶24 (“TPM was included on many enterprise-class PC and laptop...includ[ing] Dell, Lenovo, HP, Toshiba, and Fujitsu.”)

Unsupported Conjecture Regarding Mr. Kesanupalli Is Not a Stand-in for a POSITA

Here, the Board does not need to look far or make many assumptions about what a person of skill in the art would have done and why they would have done it. The Board is presented with a unique opportunity to review a reference from a contemporary POSITA—Ramesh Kesanupalli. Mr. Kesanupalli was one of the

(2024-00334) PO's Resp. (Paper 13), 16.

See also, (2024-00332) PO's Resp. (Paper 13), 15.

First, (pre-AIA) 35 U.S.C. §103(c) provides the statutory framework by which obviousness is to be determined and makes clear that obviousness is an inquiry from the perspective of a POSITA. A POSITA is an imaginary person(s), a hypothetical legal construct. The subjective decisions of Mr. Ramesh Kesanupalli, even if demonstrated unambiguously (and they are not), are not a stand-in for the legal construct of a POSITA.

(2024-00334) Pet. Reply (Paper 16), 4; see also, (2024-00334) APPL-1036, ¶¶10-13.

See also, (2024-00332) Pet. Reply (Paper 16), 2-3; (2024-00332), APPL-1030, ¶¶10-13.

Disclosed Feature Set in Kesanupalli Is Not Indicative Of Mr. Kesanupalli's Views On Combinability—Just What He (and 4 Others) Included in a Patent Application

Ex. 2037 (Goodrich Decl.) at ¶37. Mr. Kesanupalli was certainly aware of TPMs and wiping functionality and made a conscious decision to not use them in his patented system. See Section II.B.1, *supra*; Ex. 2037 (Goodrich Decl.) at ¶¶37, 60.

(2024-00334) PO's Resp. (Paper 13), 16.
See also, (2024-00332) PO's Resp. (Paper 13), 15.

patent application ≠ survey of available, compatible features

unknown. PO's assertions are simply unsupported conjecture.³ There may be any number of reasons that wiping, or a 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.

(2024-00334) Pet. Reply (Paper 16), 5.

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.

(2024-00334) APPL-1036, ¶12; cited at (2024-00334) Pet. Reply (Paper 16), 5.

Mention in Background of Kesanupalli of a Problem Does Not Constrain Obviousness Inquiry to Only Solutions Limited to That Problem

The integration of a TPM would not have helped avoid social engineering attacks. *See* Ex. 2037 (Goodrich Decl.) at ¶64. As Dr. Goodrich explains, adding a

(2024-00334) PO's Resp. (Paper 13), 21.
See also, (2024-00332) PO's Resp. (Paper 13), 20.

And the same is true for wiping functionality. As Dr. Goodrich states, "Like adding a TPM, wiping a device would have no impact on deterring a social engineering attack. Once the attacker has tricked a user to release their credentials, wiping the device will not bring those credentials back or benefit the user in anyway. . . . Simply because a POSITA could add a wipe to Kesanupalli's system does not mean it makes sense to do so." *See* Ex. 2037 (Goodrich Decl.) at ¶69.

(2024-00334) PO's Resp. (Paper 13), 23.

First, the Petition shows Kesanupalli, Brown, and Challenger are all analogous art to the '138 patent as they are in the same field of endeavor. Petition, pp. 16-17, 64-65. PO does not dispute this. Further, when more than one prior art reference is used as the basis of an obviousness rejection, it is not required that the references be analogous art to each other, much less 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).

✓ **References are analogous art, which is not disputed**

✓ **Obviousness is from POSITA's perspective**

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

Kesanupalli Is **Not** Limited to Problem of Avoiding Social Engineering Attacks

14. I have reviewed Dr. Goodrich's suggestion that U.S. Patent 8,799,666 to Kesanupalli is focused solely "on preventing social engineering attacks" and Dr. Goodrich's conclusion that, as such, Kesanupalli's teachings "would not be furthered by adding either (or both) wiping and/or a restricted interface." *See* Ex. 2037, ¶¶46, 49. I do not agree with either Dr. Goodrich's premise or his conclusion. Simply put, Kesanupalli's teachings are not constrained to *only* address or mitigate 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.

(IPR2024-00334) APPL-1036, ¶14.

See also, (IPR2024-00334) APPL-1036, ¶¶14-22; *see also* Reply, 5-9;
See also, (IPR2024-00332) APPL-1030, ¶¶14-22; *see also* Reply, 6-10.

Briefing and Expert Testimony Details Kesanupalli's Numerous Security Features Proving Protection Outside of Social Engineering Attacks

- General discussions of “**secure** transactions,” “**secure** application,” and “**secure** communication” with no implication that these are “**secure**” *only* with respect to social engineering attacks. *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 10; APPL-1036, ¶17; APPL-1006, 5:53-58, 6:15-17, 6:39-42.
- **Secure socket layer (SSL) protocol for encrypted transmission** of data including between the sensor and general processor. *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 9; APPL-1036, ¶17; APPL-1006, 1:28-30, 6:39-42.
- Strong **cryptographic algorithms** in its hardware and/or software including **cryptography features** of secure keys and hashes. *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 9; APPL-1036, ¶17; APPL-1006, 4:12-23, 4:64-5:33.
- Strengthening security by **biometric sensor unique identifiers (ID)**. *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 9; APPL-1036, ¶17; APPL-1006, 4:23-30.
- Addressed “dictionary attacks.” *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 8; APPL-1036, ¶19; APPL-1006, 1:35-38.
- Concerned with malware risk and **digitally signs its browser extensions** as mitigation and **checks credentials and biometric component**. *See, e.g.,* (2024-00334) Pet. Reply (Paper 16), 8; APPL-1036, ¶¶17-18; APPL-1006, 8:23-28.

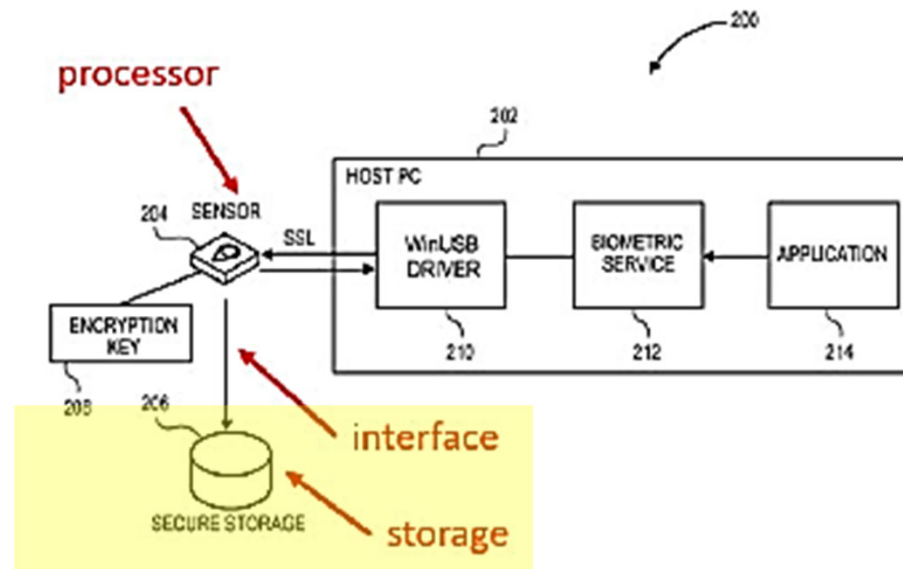
Kesanupalli Includes Device Security Features

Kesanupalli's concern was curbing social engineering attacks and not breaches to the actual device. Adding a TPM just to add a TPM would be like "gold

(2024-00334) PO's Resp. (Paper 13), 30.

See also, (2024-00332) PO's Resp. (Paper 13), 28.

Kesanupalli's
"secure storage 206"



APPL-1006, FIG. 2, annotated

(Kesanupalli), APPL-1006, FIG. 2, 3:46-51, 6:6-10; (2024-00334) Pet. (Paper 2), 24.

POSITA Would Consider Security in a Multi-Faceted Approach, Not Limited to a Single Type of Risk

POSITA's comprehensive approach to security:

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.

(2024-00334) APPL-1036, ¶122 discussed at (2024-00334) Pet. Reply (Paper 16), 12.
See also, (2024-00332) APPL-1036, ¶122 discussed at Pet. Reply (Paper 16), 10.

PO expert's undergraduate textbook:

1 Introduction	1
1.1 <u>Fundamental Concepts</u>	2
1.1.1 Confidentiality, Integrity, and Availability	3
1.1.2 Assurance, Authenticity, and Anonymity	9
1.1.3 Threats and Attacks	14
1.1.4 Security Principles	15

APPL-1032, 3 discussed at (2024-00334) Pet. Reply (Paper 16), 10;
(2024-00332) Pet. Reply (Paper 16), 12.

PO expert's testimony:

23 We discuss security principles,
24 fundamental concepts. So the concept of computer
25 security is wrapped up into a number of other
1 sub-concepts. The first three go by the initials
2 CIA, which stands for confidentiality, integrity, and
3 availability. And each of those concepts are
4 concepts of computer security.
5 And then we also, in our book, introduce
6 three additional ones, which go by AAA, which deal
7 with assurance, authenticity, and anonymity. So
8 those concepts also relate to computer security. And
9 these are all things that I teach when I teach my
10 course on computer security as being security
11 concept.

APPL-1031, 37-38 discussed at (2024-00334) Pet. Reply (Paper 16), 12;
(2024-00332), Pet. Reply (Paper 16), 10.

See also, (2024-00334) Pet. Reply (Paper 16), 12-13; APPL-1036, ¶¶20-22.
See also, (2024-00332) Pet. Reply (Paper 16), 10-11; APPL-1030, ¶¶20-22.

POSITA Would Not Limit Security Features to Just Initial Attack

⁵ PO's distinction between an attacker's *initial* strategy in exploiting a security risk—tricking human users in a social engineering attack and breaching the actual device—is untenable as these attacks are often interrelated. Social engineering attacks are often used as a precursor other exploits or intrusions of the targeted device or its resources, services or data (e.g., to deploy malware). APPL-1036, ¶21.

This is one reason why a POSITA does not approach information security and security arrangements with a goal of mitigating only one type of attack and why Kesanupalli addresses device security features in implementing its authentication techniques. APPL-1036, ¶¶22, 32 (explaining CIA and defense in depth and citing APPL-1032).

(2024-00334) Pet. Reply (Paper 16), 7.
See also, (2024-00332) Pet. Reply (Paper 16), 5.

Social engineering attacks do not exist in a vacuum, but are used as a precursor to and are related to other security risks

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).

(2024-00334) APPL-1036, ¶21 discussed at Pet. Reply (Paper 16), 7-8.
See also, (2024-00332) APPL-1030, ¶21 discussed at Pet. Reply (Paper 16), 5-7.

Kesanupalli Stores Critical Personal Information, Which Motivates Protection of the Stored Information

While Kesanupalli facilitates the 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 (which, unlike passwords, cannot be easily changed). In doing so, Kesanupalli mitigates one set of risks—weak passwords. But another risk comes to the fore—breach of the device with the password biometric information store(s). *See* APPL-1036, ¶15.

(2024-00334) Pet. Reply (Paper 16), 9; *see also*, APPL-1036, ¶15.
See also, (2024-00332) Pet. Reply (Paper 16), 7; (2024-00332) APPL-1030, ¶15.

Kesanupalli Is Ready for Improvement by Challenger's TPM-Based Architecture

to arrive at the claimed invention.”). Here, adding the TPM may increase the protection of the record locally, but Kesanupalli already had ways to protect the record and adding the TPM wouldn't have accomplished anything. *See* Response at 21-22; *See* Ex. 2037 (Goodrich Decl.) at ¶64.

(2024-00334) PO's Sur-Reply (Paper 17), 3.

See also, (2024-00332) PO's Sur-Reply (Paper 17), 10.

Dr. McDaniel's un rebutted testimony confirms Challenger's TPM-architecture augments Kesanupalli

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.

(2024-00332) APPL-1030, ¶31.

See also, (2024-00334) APPL-1036, ¶32.

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.

(2024-00332) APPL-1030, ¶32.

See also, (2024-00334) APPL-1036, ¶33.

Petition Showed Challenger Provides a Benefit of a Standards-Based Architecture that Engenders Trust

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, 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).

(2024-00332) Pet. (Paper 2), 23-24.
See also, (2024-00334) Pet. (Paper 2), 65-66.

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

(2024-00332) Pet. (Paper 2), 19-20.
See also, (2024-00332) Pet. (Paper 2), 18-24; APPL-1003, ¶¶48-51, 74-84.
See also, (2024-00334) Pet. (Paper 2), 62-66; APPL-1003, ¶¶51-54, 195-202.

Benefits of TPM Apply Regardless of Industry-Wide Adoption

First, utilizing a TPM would have introduced compatibility issues with existing systems and software that did not support TPMs. Ex. 2037 (Goodrich Decl.) at ¶66; *see* Section III.A.2, *supra*. Many security solutions that did not rely on TPMs were available and widely adopted. Ex. 2037 (Goodrich Decl.) at ¶66. Kesanupalli

(2024-00334) PO's Response (Paper 13), 32.
See also, (2024-00332) PO's Response (Paper 13), 30.

architecture. Whether or not these benefits are tempered by a lack of industry-wide adoption, this allegation does not save the patent claims from obviousness. *See KSR*, 550 U.S. at 403 (“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].”)

(2024-00334) Pet. Reply (Paper 16), 20.
See also, (2024-00332) Pet. Reply (Paper 16), 16.

TPM Was Deployed in Available Commercial Products

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.

(2024-00334) APPL-1036, ¶25 discussed at Pet. Reply (Paper 16), 18-19.

See also, (2024-00332) APPL-1030, ¶24 discussed at Pet. Reply (Paper 16), 14-15.

LAPTOPS AND NETBOOKS REVIEW

Lenovo ThinkPad T60p review

A business workhorse that offers a decent battery life and great keyboard

Our Score

User Score Be first to review this!

Last reviewed: May 4th 2008

A pleasure to use

When it comes to extra features, you'll find the standard array of tools on offer. The VGA-out port allows for connection to analogue displays and instead of an ExpressCard slot you'll find the old PC Card connection.

On the right-hand side you'll find a DVD rewriter. With 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.

(2024-00332) APPL-1033, 1; APPL-1030, ¶26, Pet. Reply (Paper 16), 14-15.

See also, (2024-00334) APPL-1033, 1; APPL-1036, ¶27, Pet. Reply (Paper 16), 18.

Discussion Roadmap

- '138 Patent Grounds:
 - Prior Art Teachings Not Seriously Disputed Slides 7-14
 - Motivation to Combine Kesanupalli and Brown Slides 21-33
 - Motivation to Combine Kesanupalli-Brown and Challenger Slides 21-37
- '512 Patent Grounds:
 - Prior Art Teachings Not Seriously Disputed Slides 15-19
 - Motivation to Combine Kesanupalli-Cheng and Challenger Slides 21-37
 - Petition demonstrates “*a second processor is configured to: ... perform a secure backup of the record to a storage service*” Slides 39-49

Parties Appear to Agree that Claims Recite “*the second processor is configured to...perform a secure backup of the record to a storage service*”

Petition demonstrates that POSITA would have been motivated to configure Kesanupalli-Challener’s *second (secure) processor to perform a secure backup of the record to a storage service*

1. A system, comprising:
 - a first processor of a first device, 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; and
 - communicate with a second processor using a restricted interface, wherein **the second processor is configured to:**
 - ...**
 - 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; and
 - a memory coupled to the first processor and configured to provide the first processor with instructions.
2. The system recited in claim 1, wherein the storage service comprises **a cloud storage service.**

(’512 Patent, claims 1-2)
APPL-1001, 10:62-11:33.

Petition Explains *Second Processor* Perform[s] Secure Backup

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

(2024-00332) Pet. (Paper 2), 55.

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).

(2024-00332) Pet. (Paper 2), 55; *see also*, APPL-1003, ¶¶158-164, 173.

Cheng teaches *secure backup* by encrypting data of a biometrics-based device and providing it to a storage service

It would have been obvious to implement Cheng's backup on Kesanupalli-Challener's *second (secure) processor*

- data relates to security features
- secure processor is protected from attacks
- records are accessible only to secure processor

Arrangement was conventional and implemented by widely practiced methods

Implementation of *Second Processor* Perform[ing] Secure Backup Is Well-Supported

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.

Petition details how the *second processor* performs the secure backup including:

- Backup in context of TPM was known in industry (APPL-1018)
- Porting of code to second processor described
- Cheng itself teaches using a microprocessor onboard a biometric-based device (*second processor*)

(2024-00332) Pet. Reply (Paper 16), 18-19.
See also, (2024-00332) Pet. (Paper 2), 54-59, APPL-1003, ¶¶158-164, 173.

Dr. McDaniel's Confirms that it Was Straight-Forward for *Second Processor* to Perform Cheng's *Secure Backup*

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

(2024-00332) APPL-1030, ¶36 discussed at Pet. Reply (Paper 16), 18-19.

TPM-based Architecture Restricts Access to the *Second Processor*

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).

(2024-00332) Pet. Reply (Paper 16), 20.

Cheng's backup technique implements security features such as encryption, which are provided by the *second (secure) processor*

- **Restricted interface keeps *second processor* secure**
- **However, the *second (secure) processor* can interact with outside world through the restricted interface**

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).

(2024-00332) APPL-1030, ¶37 discussed at Pet. Reply (Paper 16), 20.

Claims Recite “the second processor is configured to...perform a secure backup of the record to a storage service”

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, wherein the second processor is configured to:
...
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.
2. The system recited in claim 1, wherein the storage service comprises a cloud storage service.

Patent Owner’s arguments fail as they demand an unsupported claim interpretation :

a second processor configured to
“perform” a secure backup precludes
downstream components along path
to cloud storage service

(’512 Patent, claims 1, 2)
APPL-1001, 10:62-11:33.

Claim Language Does Not Preclude Involvement of Downstream Components

1. A system, comprising:
a first processor of a first device, 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; and
communicate with a second processor using a restricted interface, 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
access a record stored in a secure storage, wherein the record is associated at least with the external resource;
retrieve, from the record, at least one of a password, a cookie, or a cryptographic key;
perform a cryptographic operation;
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
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; and
a memory coupled to the first processor and configured to provide the first processor with instructions.

('512 Patent, claim 1) APPL-1001, 10:62-11:31.

Recitation of “facilitate a login” does not transform the meaning of “perform” to preclude downstream components

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.

(2024-00332) APPL-1030, ¶41 discussed at Pet. Reply (Paper 16), 25.

Secure Backup to Remote Storage Service Uses Downstream Components

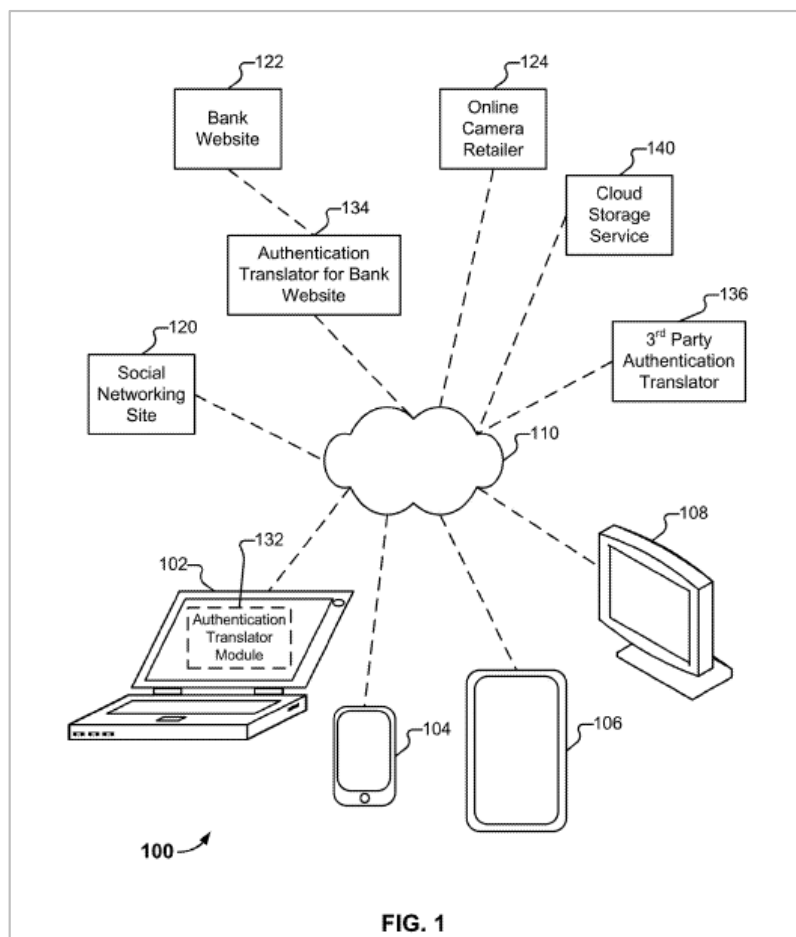


FIG. 1

('512 Patent) APPL-1001, FIG. 1, discussed at Pet. Reply (Paper 16), 24-25.
Pet. (Paper 2), 3-4; APPL-1001, 11:32-33 (claim 2).

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.

(2024-00332) APPL-1030, ¶38 discussed at Pet. Reply (Paper 16), 24-25.

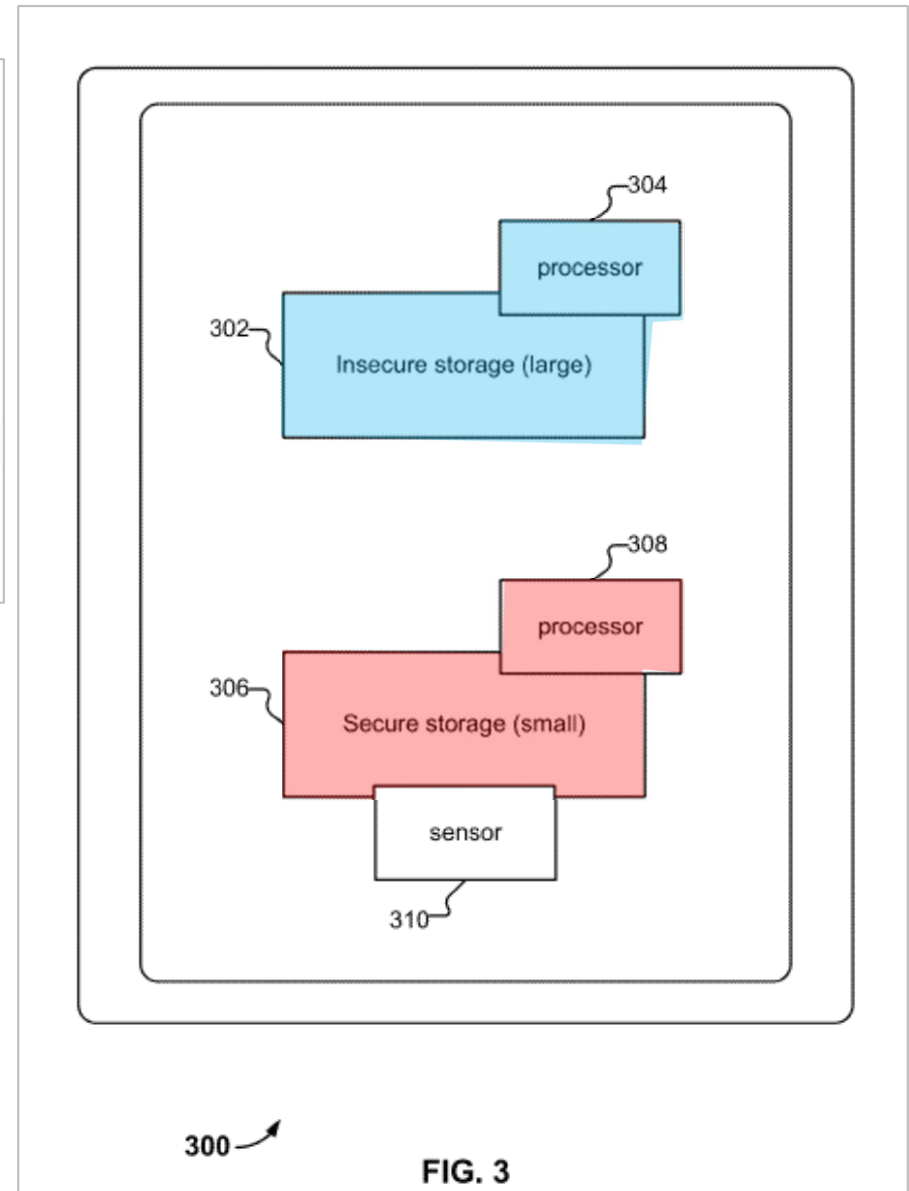
Second Processor Communicates with the First Processor

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

APPL-1001, 3:66-4:8 discussed at Pet. Reply (Paper 16), 21-22.

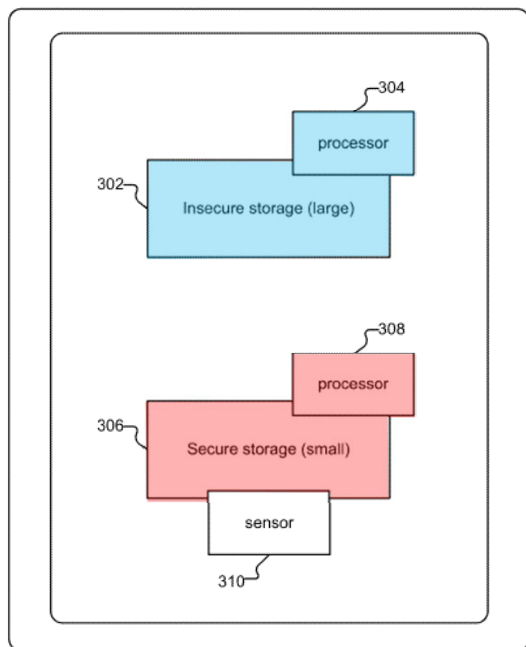
Patent Owner's expert agreed the communication path to the second processor is via a restricted interface with the first processor

(2024-00332) Pet. Reply (Paper 16), 21-23 citing APPL-1031, 35-36.



APPL-1001, FIG. 3 discussed at Pet. Reply (Paper 16), 21-22.
See also, Pet. (Paper 2), 7.

'512 Patent Describes “Backup” Path from Second Processor through Insecure Storage of *First Processor*



'512 Patent Backup Process:

1. record accessed by **second processor**
2. encrypted by **second processor**
3. written by **second processor** to **insecure storage of first processor**
4. “in turn propagate[d]” to external backup storage

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

(2024-00332) APPL-1030, ¶39 discussed at Pet. Reply (Paper 16), 21-24.

The Only Identified Embodiment in the '512 Patent is a Communication Path Including a First Processor

Petitioner fails to acknowledge that every embodiment in the '512 Patent might not be claimed by these specific claims. Just because the backup method may include the first processor in some embodiments, does not mean that the present claims require the same. *MySpace*, 672 F.3d at 1256; *Johnson & Johnston*, 285 F.3d at 1053. A patent's claims need not cover every embodiment disclosed in the

(2024-00332) PO Sur-Reply (Paper 17), 5.

	'512 Patent	Evidentiary Support
<i>second processor</i> communication path <u>includes</u> downstream component(s)	 APPL-1001, Fig. 3, 3:66-4:12 APPL-1001, Fig. 1	 APPL-1030, ¶¶37-39 APPL-1031, 35-36
<i>second processor</i> communication path <u>precludes</u> downstream component(s)		

(2024-00332), Pet. Reply (Paper 16), 21-26, APPL-1030, ¶¶36-42.
See, e.g., (2024-00332) PO Sur-Reply (Paper 17), 5-6.

Summary Of Conclusions — '138 Patent

- | | | |
|--|--------------------|---|
| • Prior Art Teaching of Claim Elements | Uncontested | ✓ |
| • Motivation to Combine Kesanupalli and Brown | Unrefuted | ✓ |
| • Motivation to Combine Kesanupalli-Brown and Challenger | Unrefuted | ✓ |

- Patent Owner's Reasons Not to Combine

Contrary to Legal Standards
§103 and *KSR*

X

Summary Of Conclusions — '512 Patent

- Prior Art Teaching of Claim Elements
- Motivation to Combine Kesanupalli-Cheng and Challenger
- Petition demonstration that “*a second processor is configured to: ... perform a secure backup of the record to a storage service*”

Uncontested



Unrefuted



Unrefuted



- Patent Owner’s argument that the “*second processor is configured to: ... perform a secure backup of the record to a storage service*” precludes downstream component(s)

Unpersuasive
Contrary to '512
Patent Claims and
Specification



Thank You