

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

AIRE TECHNOLOGY LIMITED,
Patent Owner.

IPR2022-01135
Patent 8,205,249 B2

Before MIRIAM L. QUINN, JEFFREY S. SMITH, and
BRIAN J. McNAMARA, *Administrative Patent Judges*.

SMITH, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining All Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

Petitioner, Apple Inc., filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1–12 of U.S. Patent No. 8,205,249 B2 (Ex. 1001, “the ’249 patent”) pursuant to 35 U.S.C. § 311(a). Patent Owner, Aire Technology Ltd., filed a Response (Paper 14, “PO Resp.”). Petitioner filed a Reply (Paper 15, “Pet. Reply”), and Patent Owner filed a Sur-Reply (Paper 23, “PO Sur-Reply”). A hearing was held on October 2, 2023.

We have jurisdiction to conduct this *inter partes* review under 35 U.S.C. § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a). For the reasons discussed below, we determine claims 1–12 are unpatentable.

II. REAL PARTIES-IN-INTEREST

Petitioner identifies itself (Apple, Inc.) as its sole real party-in-interest. Pet. 68. Patent Owner identifies itself (Aire Technology Ltd.) as its sole real party-in-interest. Paper 4, 2.

III. RELATED MATTERS

The Petition states that the ’249 patent is the subject of the following proceedings:

Aire Technology Ltd. v. Google LLC, No. 6-21-01104, W.D. Tex., filed Oct. 25, 2021;

Aire Technology Ltd. v. Apple, Inc., No. 6-21-01101, W.D. Tex., filed Oct. 22, 2021 (“the Apple litigation”);

Aire Technology Ltd. v. Samsung Electronics co, Ltd. et al., No. 6-21-00955 W. D. Tex., filed Sep. 15, 2021;

Samsung Electronics Co., Ltd. v. Aire Technology Ltd., IPR2022-00875 (PTAB, Apr. 22, 2022)

IPR2022-01135
Patent 8,205,249 B2

Pet. 68. Patent Owner identifies the following additional proceedings as
“related current and/or former proceedings involving the patent at issue.”
Paper 4, 2–3.

Samsung Electronics Co., Ltd. v. Aire Technology Ltd.,
IPR2022-00874 (PTAB April 22, 2022)

Samsung Electronics Co., Ltd. v. Aire Technology Ltd.,
IPR2022-00876 (PTAB May 2, 2022);

Samsung Electronics Co., Ltd. v. Aire Technology Ltd.,
IPR2022-00877 (PTAB May 2, 2022);

Apple Inc. v. Aire Technology Ltd., IPR2022-01136 (PTAB June 15,
2022);

Apple Inc. v. Aire Technology Ltd., IPR2022-01137 (PTAB June 15,
2022).

IV. THE '249 PATENT

The '249 patent generally relates to “secure authentication of a user of
a portable data carrier communicating with a terminal.” Ex. 1001, 1:9–10.
A user uses the portable data carrier to perform a secure electronic
transaction with the terminal. *Id.* at 3:3–9, Abstract. Fig. 1 of the '249
patent, shown below, illustrates the portable data carrier and the terminal.

Fig. 1

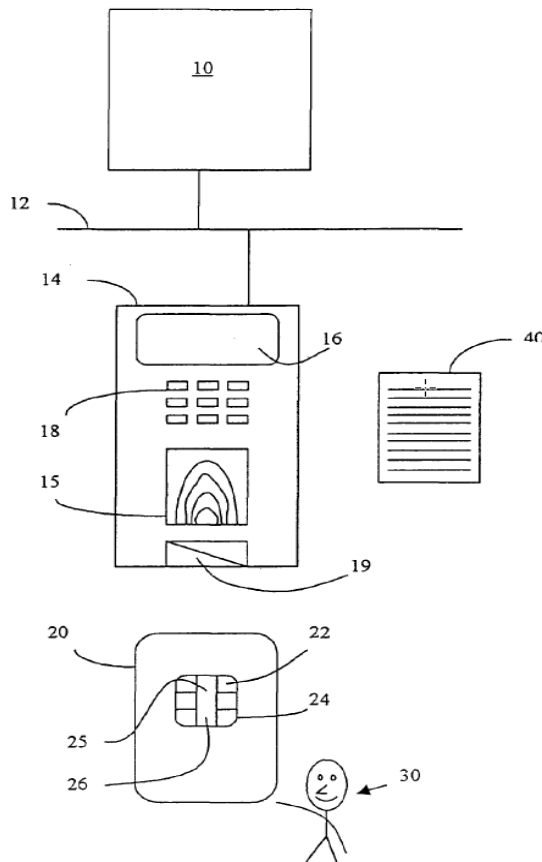


Figure 1 above illustrates a structure of a transaction system for effecting a secure electronic transaction. Ex. 1001, 3:17–18. Data network 12 exchanges data between terminal 14 and background system 10. *Id.* at 3:42–43. Terminal 14 includes display screen 16 and input means 18. *Id.* at 4:46–49. Terminal 14 includes interface 19 for communicating with portable data carrier 20. Terminal 14 includes sensor device 15 for detecting a biometric feature such as a fingerprint of user 30. *Id.* at 4:57–61.

The '249 patent explains that the “portable data carrier 20 is further set up to perform ... a plurality of different quality user authentication methods.” Ex. 1001, 3:22–26. For example, the portable data carrier “expediently supports at least one knowledge-based authentication method, e.g., a PIN check, and at least one biometric method.” *Id.* at 3:26–28. The

'249 patent notes that the “biometric method inherently constitutes the higher-quality one here, since it presupposes the personal presence of the user 30; this is not ensured in the knowledge-based method since the knowledge can have been acquired by an unauthorized user.” *Id.* at 3:29–34.

When performing a secure electronic transaction, the portable data carrier receives either the PIN or biometric, e.g., fingerprint, input by the user and either “checks the transmitted PIN” or “compares the received extracted [fingerprint] features with the reference features stored in the storage means and checks whether a sufficient match is present.” Ex.1001, 4:19–64. If the PIN or fingerprint is a match with the stored values, the portable data carrier “confirms the correctness to the terminal.” *Id.* at 4:27–28, 4:64–67. Then, the portable data carrier “perform[s] the security-establishing operation, i.e., the digital signature.” *Id.* at 4:30–32, 5:1–6. The portable data carrier also “forms quality information,” where the “quality information [is] about the quality of the previously performed user authentication.” *Id.* at 5:15–17, 5:39–41. Then, a “security message consisting of digital signature and quality information is sent by the portable data carrier 20 back to the terminal 14.” *Id.* at 5:21–23.

V. ILLUSTRATIVE CLAIM

Challenged claim 1 of the '249 patent recites:

[1.0] A method for effecting a secure electronic transaction on a terminal

[1.1] using a portable data carrier arranged to perform different quality user authentication methods,

[1.2] wherein the portable data carrier performs a user authentication using one of said different user authentication methods, the portable data carrier confirms the proof of authentication to the terminal, and

[1.3] the portable data carrier then performs a security establishing operation within the electronic transaction,

[1.4] comprising the steps of creating authentication quality information by the portable data carrier about said user authentication method used and

[1.5] attaching said authentication quality information to the result of the security-establishing operation,

[1.6] wherein the difference in quality of said user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective.

VI. ASSERTED GROUNDS

Petitioner asserts that claims 1–12 of the '249 patent are unpatentable on the following ground.

Claim(s) Challenged	35 U.S.C. § ¹	Reference(s)/Basis
1–12	103(a)	Burger ² , Cheng ³

VII. LEVEL OF ORDINARY SKILL

Petitioner identifies a person of ordinary skill as someone knowledgeable and familiar with the secure electronic transaction arts. Pet. 13. Petitioner states that such a person “would have at least a four-year degree in electrical engineering, computer engineering, computer science, or a related field and two years of relevant experience in computer security, and developing, implementing, or deploying portable devices on systems connected to computer networks. A Master’s or Ph.D. degree in a relevant

¹ The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011) (“AIA”), amended 35 U.S.C. § 103. Because the '249 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

² U.S. Patent No. 7,080,037 B2; iss. July 18, 2006 (Ex. 1005).

³ U.S. Publication No. 2004/0039909 A1; pub. Feb. 26, 2004 (Ex. 1006).

field may substitute for some work experience and greater experience might substitute for a four-year degree.” *Id.* Patent Owner does not address the level of ordinary skill. *See generally*, PO Resp.

The level of ordinary skill in the art usually is evidenced by the references themselves. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

As Petitioner’s description of a person of ordinary skill appears commensurate with the subject matter before us, we apply Petitioner’s definition for purposes of this Decision.

VIII. CLAIM CONSTRUCTION

We interpret claim terms using “the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b).” 37 C.F.R. § 42.100(b) (2019). In this context, claim terms “are generally given their ordinary and customary meaning” as understood by a person of ordinary skill in the art in question at the time of the invention. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (citations omitted) (en banc). “In determining the meaning of the disputed claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17). Extrinsic evidence is “less significant than the intrinsic record in determining ‘the legally operative meaning of claim language.’” *Phillips*, 415 F.3d at 1317 (citations omitted).

We construe only those claim terms that require analysis to determine whether to institute inter partes review. *See Vivid Techs., Inc. v. Am. Sci. &*

Eng'g, Inc., 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that “only those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy”). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994).

Petitioner acknowledges that in parallel district court litigation, it has proposed the term “an inherently relatively lower quality and an inherently relatively higher quality from a security perspective” recited in claims 1 and 10 be construed as indefinite. Pet. 15. Noting that in the district court, Patent Owner asserted no construction is necessary, Petitioner adopts Patent Owner’s district court proposed construction for purposes of this proceeding. *Id.* We agree that no construction of this term is necessary, as the plain and ordinary meaning of “an inherently relatively lower quality and an inherently relatively higher quality from a security perspective” is ascertainable in the context of the claims.

Claim 1 recites “the portable data carrier then performs a security-establishing operation within the electronic transaction, comprising the steps of creating authentication quality information by the portable data carrier about said user authentication method used and attaching said authentication quality information to the result of the security-establishing operation.” Claim 10 recites similar limitations. Patent Owner contends that these limitations require a portable data carrier to separately perform a security establishing operation within an electronic transaction and then to attach quality information about the user authentication method to the result of the security-establishing operation. PO Resp. 11. Patent Owner contends that the quality information and the result of the security-establishing operation

must be attached prior to communicating the information and result to another device. *Id.* Patent Owner contends that “the ’249 patent describes an exemplary ‘security-establishing operation’ of creating a digital signature of an electronic document.” *Id.* (citing Ex. 1001, 5:11–13). Thus, under Patent Owner’s proposed construction, the claimed “security establishing operation,” read in light of the specification, encompasses the example of creating a digital signature, but is not limited to creating a digital signature. Patent Owner contends that the purpose of the security-establishing operation is to confirm aspects of a commercial transaction, such as signing sales orders, and that the quality information is joined with the digital signature to be securely communicated to the other party in the transaction. *Id.* at 12 (citing Ex. 1001, 1:27–30, 5:16–26, 5:32–39).

Petitioner contends that we do not need to construe this claim term, because the prior art teaches this claim term under Patent Owner’s construction and under the plain meaning of the claims. Pet. Reply. 2. Patent Owner disagrees, contending that this claim term recites that the claimed “security-establishing operation” is performed “within [a secure] electronic transaction,” which means that the claims are expressly directed to the security of the transaction. PO Sur-Reply 9. According to Patent Owner, the claimed “security-establishing operation” is performed to establish, confirm, or authenticate aspects of a commercial transaction, such as signing sales orders. *Id.* at 10 (citing Ex. 1001, 1:27–30). Patent Owner contends that the scope of establishing security within a transaction by using a digital signature does not encompass encrypting the digital signature. *Id.* at 10–11.

We disagree with Patent Owner’s proposal to limit the “security-establishing operation” to a digital signature that establishes, confirms, or

authenticates aspects of a commercial transaction, and the intrinsic record does not express “a clear indication . . . that the patentee intended the claims to be so limited.” *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1327 (Fed. Cir. 2012); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1323 (Fed. Cir. 2005) (en banc) (“[C]laims may embrace different subject matter than is illustrated in the specific embodiments in the specification.”). Rather, we agree with Patent Owner, that “an exemplary ‘security establishing operation’ [is] creating a digital signature.” PO Resp. 11; Ex. 1001, 4:31–32 (“the chip card . . . perform[s] the security-establishing operation, i.e., the digital signature”); 4:67–5:2 (“the portable data carrier 20 switches itself ready to execute the intended security-establishing operation, i.e., perform a digital signature”). Therefore, the claimed “security-establishing operation” is not limited to an operation that creates a digital signature.

We are not persuaded by Patent Owner’s argument that the “security-establishing operation” excludes other operations that establish security, such as encryption operations generally. The specification’s description of a digital signature (Ex. 1001, 4:31–32, 4:67–5:2) as a way to perform the “security-establishing operation,” in no way indicates that a further encryption of a digital signature is precluded as a way to carry out the recited operation.

We are also not persuaded by Patent Owner’s argument that, because the “security-establishing operation” must be performed “within the electronic transaction,” the claimed operation cannot encompass secured communication by the data carrier. PO Sur-reply 1 (arguing that the “[t]he ’249 patent teaches and claims a portable data carrier that performs a ‘security establishing operation’ inside the transaction and separate from the

secure communication mechanism of the data carrier.”); *see also* PO Sur-reply 9–11. The claim language does not make any distinctions between security of data carrier communications and security of the electronic transaction itself. In other words, the claim language is agnostic as to whether the electronic transaction is securely established by performing a digital signature of a transaction document or by encrypting the transmission of the document. Again, we recognize that the ’249 patent specification describes the data carrier’s operation as performing a digital signature, as stated above. But this one embodiment is not limiting. The specification broadly describes one *example* of the microprocessor in the data carrier as capable of subjecting a data record to a “cryptographic algorithm.”

Ex. 1001, 3:16–19. There is no indication in this embodiment of a “security-establishing operation” or in the claim language, that the cryptographic algorithm must be applied at any particular time, such that the security-establishing operation cannot be an encryption operation concurrent with secured transmissions by the data carrier.

Therefore, based on the evidence of record, we construe “creating authentication quality information by the portable data carrier about said user authentication method used and attaching said authentication quality information to the result of the security-establishing operation” to encompass at least attaching quality information to an encrypted document, such as a digitally signed document.

In addition, for the reasons given below in our unpatentability analysis, we agree with Petitioner, that under either Petitioner’s construction or Patent Owner’s construction, the prior art relied on in the Petition teaches “the portable data carrier then performs a security-establishing operation within the electronic transaction, comprising the steps of creating

authentication quality information by the portable data carrier about said user authentication method used and attaching said authentication quality information to the result of the security-establishing operation,” as claimed.

IX. ANALYSIS

A. *Legal Standards*

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable.” *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the challenge to each claim”)); *see also* 37 C.F.R. § 42.104(b) (requiring a petition for *inter partes* review to identify how the challenged claim is to be construed and where each element of the claim is found in the prior art patents or printed publications relied upon).

A claim is unpatentable under 35 U.S.C. § 103(a) if “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective evidence of obviousness or nonobviousness, i.e., secondary considerations.⁴ *See*

⁴ The parties do not direct us to any objective evidence of non-obviousness at this stage of the proceeding.

Graham v. John Deere Co., 383 U.S. 1, 17–18 (1966). An obviousness analysis “need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” *KSR*, 550 U.S. at 418.

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2016) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)). Furthermore, Petitioner does not satisfy its burden of proving obviousness by employing “mere conclusory statements,” but “must instead articulate specific reasoning, based on evidence of record, to support the legal conclusion of obviousness.” *In re Magnum Oil Tools Int’l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

B. Claims 1–12 As Obvious Over Burger and Cheng

1. Burger – Exhibit 1005

Burger describes a “hand-held portable electronic authorization device” (called a Pocket Vault) that is used to carry out electronic financial transactions with a terminal such as a point-of-sale or commercial interface station. Ex. 1005, 1:17–19, 8:38–47, 2:42–50. The Pocket Vault stores electronic versions of the contents of a user’s wallet, such as credit cards, driver’s license, library card, and frequent flyer card. *Id.* at 11:37–47. When the Pocket Vault is powered on and prior to any transaction, Pocket Vault authenticates the holder of the device using one or more of a plurality of different authentication methods. Ex. 1005, 12:6–25, 22:36–52. For example, the Pocket Vault may perform an “analysis of a biometric feature

of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.).” *Id.* at 12:9–16, 19:41–53, 17:50–67. “Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder’s identity.” *Id.* at 12:16–18. After authentication, the Pocket Vault transmits an encrypted message, including the Pocket Vault ID, to the commercial interface station. *Id.* at 23:13–19.

The holder may then choose to “invoke a wireless transaction” with the interface station. Ex. 1005, 23:65–24:6, 29:40–43, 30:6–21, 2:42–50. Burger explains that when the Pocket Vault “communicate[s]” with the commercial interface station as part of the wireless transaction, it performs PKI-based security establishing operations “well known in the art” to secure the communications. *Id.* at 55:29–35, 12:37–51.

2. *Cheng – Exhibit 1006*

Cheng describes a “portable authentication device” carried by an authorizee and configured for use in electronic transactions, such as “transactions through a bank machine.” Ex. 1006 ¶¶ 10, 31, 39. The portable authentication device is configured to authenticate the holder of the device through a variety of authentication methods (called “authentication factors”) performed on the device, including non-biometric factors such as a PIN code or a password, and biometric factors such as a fingerprint or facial recognition. *Id.* ¶¶ 43, 34. Cheng explains that a user of the device is permitted to select from or delete the various alternative authentication factors. *Id.* ¶ 38.

Cheng discloses associating different authentication factors with different levels of authentication, where authentication factors within the same level represent the same quality of authentication. Ex. 1006 ¶¶ 32–35.

Cheng explains that “[a]n increasing level of authentication is associated with an increasing level of confidence in security.” *Id.* ¶ 33. For example, an authentication method based on an individual’s fingerprint has a higher authentication level, or quality, than an authentication method based on a PIN code. *Id.* ¶ 34.

Cheng provides an example of different authentication levels and associated authentication methods in Table 1 reproduced below:

TABLE 1	
Authentication Level	Authentication Factor(s)
Authentication Level 1	Possession
Authentication Level 2	PIN
Authentication Level 3	Any external supplied biometrics factors
Authentication Level 4	Two external supplied biometrics factors or on-board fingerprint
Authentication Level 5	Any external supplied biometrics plus on-board fingerprint or PIN, or on-board Multi-digit fingerprint with 2 out of 3 minimum
Authentication Level 6	Two external supplied biometrics plus on-board fingerprint or PIN, or on-board Multi-digit fingerprint with 3 out of 5 minimum
Authentication Level 7	On-board multi-digit, digit specific, complete match plus PIN

Cheng discloses that when several authentication methods are available to a user, an authorizer of a transaction, such as a vendor, may select a specific authorization level required for that transaction. Ex. 1006 ¶¶ 3, 5, 37. For example, for a certain transaction, the authorizer may require that the authorizee, or user of the device, use an authentication method corresponding to authentication level 3. *Id.* ¶¶ 34, 37. In this case, the authorizee would be granted access only if the authorizee uses an authentication method of at least level 3. *Id.* ¶¶ 11, 36.

3. Reasons to Combine the Teachings of Burger and Cheng

Petitioner contends a person of ordinary skill would have had reason to combine the teachings of Burger and Cole because both references concern methods for performing secure electronic transactions with a

portable authentication device and the combination would allow a point-of-sale terminal performing such a transaction with Burger's Pocket Vault to accurately gauge the security risk of the transaction by receiving information about how the user of the Pocket Vault was authenticated as taught by Cheng. Pet. 32–36 (citing Ex. 1003, Neuman Decl. ¶¶ 50, 52–60). Petitioner contends that a person of ordinary skill would have had a reasonable expectation of success because Cheng's technique was specifically intended to be implemented in a portable authentication device such as Burger's Pocket Vault. Pet. 36–37 (citing Ex. 1003, Neuman Decl. ¶ 61).

Burger teaches a handheld portable electronic device that authenticates a user with one of a plurality of authentication methods of varying quality when carrying out a transaction with a point-of-sale terminal. Ex. 1005, 1:17-19, 2:42-59, 12:6-27, 23:65-24-6. Cheng teaches a portable authentication device that communicates authentication quality information to an authorizer when carrying out a transaction. Ex. 1006 ¶¶ 36, 45; *see id.* at Abstract, ¶¶ 33-34, 46. We find that person of ordinary skill would have provided authentication method quality information to an authorizer such as a point-of-sale terminal as taught by Cheng when carrying out a transaction using Burger's electronic device to yield the benefit of enabling the point-of-sale terminal to better gauge the risk of the transaction, so that relatively low-value transactions may be authenticated to a lower level of confidence, and relatively high-value transactions may be authenticated to a higher level of confidence, before allowing the transaction to proceed. Ex. 1003 ¶¶ 57, 60; Ex. 1008, 73:15-21; Ex. 1009, 13:41-53.

4. *Claims 1 and 10*

1.0 A method for effecting a secure electronic transaction

The preamble of claim 1 recites a “method for effecting a secure electronic transaction to a terminal.” Petitioner contends that Burger discloses this section of the preamble in describing methods for performing electronic transactions between a handheld Pocket Vault and a point-of-sale or other commercial interface station. Pet. 38 (citing Ex. 1005, 1:17–19, 8:38–47, 2:42–50). Petitioner contends that such transactions are secure because the user of the Pocket Vault is authenticated with each attempted use, and communications between the Pocket Vault and other devices are encrypted. *Id.* at 39 (citing Ex. 1005, 12:6–27, 12:40–50, 55:29–35). Patent Owner does not dispute Petitioner’s contentions. We agree with Petitioner, that Burger teaches this section of the preamble of claim 1, for the reasons given in the Petition.

1.1 using a portable data carrier

The preamble of claim 1 recites “using a portable data carrier arranged to perform different quality user authentication methods.” The preamble of claim 10 recites “arranged to perform different quality user methods.” Petitioner contends that Burger discloses these sections of the preambles of claims 1 and 10 in describing a Pocket Vault arranged to perform different authentication methods such as PIN-based methods and biometric-based methods. Pet. 40–41 (citing Ex. 1005, 12:6–25, 15:24–41, 17:50–67, 19:41–53, Fig. 26E), 65. Petitioner contends that Cheng also discloses these sections of the preambles in describing different authentication methods associated with different levels of quality. *Id.* at 41–42 (citing Ex. 1006 ¶¶ 33–34, table 1). Patent Owner does not dispute Petitioner’s contentions. We agree with Petitioner, that the combination of

Burger and Cheng teaches these sections of the preambles of claims 1 and 10, for the reasons given in the Petition.

1.2 wherein the portable data carrier performs

The preamble of claim 1 recites “wherein the portable data carrier performs a user authentication using one of said different user authentication methods, the portable data carrier confirms the proof of authentication to the terminal.” Claim 10 recites “the portable data carrier is arranged to perform a user authentication using one of said implemented user authentication methods and the portable data carrier is arranged to confirm the authentication to a terminal.” Petitioner contends that Burger discloses this section of the preamble of claim 1 and this limitation of claim 10 in describing a fingerprint scanner that scans the fingerprint of the Pocket Vault holder, determines whether the scanned fingerprint matches a stored fingerprint, and if so, transmits an encrypted message confirming authentication to the commercial interface station. Pet. 42–43 (citing Ex. 1005, 22:36–52, 23:1–4, 23:13–19, 18:10–24, Figs. 3 and 7), 65–66. Patent Owner does not dispute Petitioner’s contentions. We agree with Petitioner, that Burger teaches this section of the preamble of claim 1 and this limitation of claim 10, for the reasons given in the Petition.

1.3 perform[ing] a security-establishing operation

The preamble of claim 1 recites “the portable data carrier then performs a security establishing operation within the electronic transaction.” The preamble of claim 10 recites a “portable data carrier for performing a security-establishing operation within a secure electronic transaction.” Petitioner contends that the combination of Burger and Cheng teaches these sections of the preambles of claims 1 and 10. Pet. 45–48, 65. Petitioner contends that Burger discloses a method of performing a wireless transaction

by encrypting communications between the Pocket Vault and the commercial interface station. *Id.* at 45–48 (citing Ex. 1005, 2:51–59, 12:37–51, 23:60–24:6, 29:40–43, 30:6–21, 55:23–27, Figs. 7 and 10). Petitioner contends that Cheng discloses a portable authentication device that performs a digital signature to establish secured communication. *Id.* at 48 (citing Ex. 1006 ¶ 44).

Patent Owner contends that the '249 patent discloses the claimed “security-establishing operation” as a digital signature that secures a transaction in a manner that is distinct from securing communications between parties, and makes it possible to effect particularly security-critical transactions, such as placing service orders involving costs. PO Resp. 12-13 (citing Ex. 1001, 1:27–30, 3:44–45, 4:24–26, 5:10–15). Patent Owner contends that Burger and Cheng, in contrast, teach encrypted communications between an authentication device and a terminal. *Id.* at 13–14. Patent Owner further contends that Cheng does not disclose using a digital signature as part of the security-establishing operation as described by the '249 patent. *Id.* at 15 (citing Ex. 1001, 3:16–20, 3:44–45, 5:9–15). According to Patent Owner, Cheng teaches using the digital signature to establish secured communications between an authentication device and another device. *Id.*

Petitioner contends that Burger teaches securing of authentication and communications using techniques well known in the art, and that one such well known security establishing operation was performing a digital signature as taught by Cheng. Pet. Reply 9 (citing Pet. 47–48; Ex. 1005, 55:23–35, 12:37–51; Ex. 1006 ¶ 44; Ex. 1003 ¶ 81; Ex. 1010, 9:59–10:4; Ex. 1007 ¶ 24; Ex. 1011, 1:6–31, 2:1–14, 4:16–22). Petitioner contends that the combination of Burger and Cheng therefore teaches “performing a security-

establishing operation” that is explicitly within the scope of the claim. *Id.* at 10. Petitioner contends that securing the communicated information within a transaction as taught by the combination of Burger and Cheng is securing the transaction within the scope of the claim. *Id.* at 10-11. In particular, Petitioner contends that the security-establishing operation described in the ’249 patent, namely, performing a digital signature, is the same type of security-establishing operation taught by the combination of Burger and Cheng, performed within the same type of transaction, using the same type of transaction system. *Id.* at 11–12.

Patent Owner contends that the claimed “security-establishing operation” is performed “within [a secure] electronic transaction,” which means that the claims are directed to the security of the transaction and not the mechanisms used to communicate the details of the transaction. PO Sur-Reply 8–9. Patent Owner contends that the claimed “security-establishing operation” is performed to establish, confirm, or authenticate aspects of a commercial transaction, such as signing sales orders. *Id.* at 10. According to Patent Owner, the claimed “security-establishing operation” of a digital signature could be transferred without employing an encrypted communication system. *Id.* at 11. Patent Owner contends that the secure encrypted communications between an authentication device and a terminal as taught by the combination of Burger and Cheng does not teach a “security-establishing operation” within a transaction as claimed. *Id.* at 12.

Patent Owner further contends that the Petition does not offer any expert-supported positions, because the testimony of Dr. Neuman is either identical, nearly identical, or substantially identical to the Petition. PO Sur-Reply 3. Patent Owner contends that even though the opinions that Dr. Neuman submitted in his declarations were his own, the declarations were

initially drafted by attorneys. *Id.* Patent Owner contends that Dr. Neuman does not cite to any additional supporting evidence or provide any technical reasoning to support his statements, all of which bear the hallmark of being copied and pasted from the draft of the Petition. *Id.* at 34 (citing *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022)); *see id.* at 47.

We are not persuaded by Patent Owner's argument that we should accord the testimony of Dr. Neuman little or no weight simply because it is identical to what Petitioner states in the Petition. The *Xerox* case cited by Patent Owner does not require or indicate otherwise. *See Xerox* at 1517 (noting that the deficiencies with expert testimony are that they are conclusory and lacking supporting evidence or technical reasoning.). Mr. Neuman's testimony apprises us of why one of ordinary skill in the art would have understood the assertions made in the Petition, and his testimony is supported by evidence. For example, in testifying that performing a digital signature was one known security operation used to secure transaction communications, Dr. Neuman supports his testimony with evidence from Cheng, Sarcanin, Russo, and Fischer. Ex. 1003 ¶ 81 (citing Exs. 1006, 1007, 1010, and 1011). We find that the declarations of Dr. Neuman are based on specific factual disclosures in the evidence of record. Therefore, we credit Dr. Neuman's declaration testimony for the matters asserted based on the evidence and technical reasoning provided therein.

We agree with Petitioner, that securing the communicated information within a transaction as taught by the combination of Burger and Cheng teaches securing the transaction within the scope of the claim. Pet. Reply 10. In particular, we agree that, even under Patent Owner's narrower construction, Cheng's digital signature that establishes security teaches the

claimed “security-establishing operation” as read in light of the specification. *Id.* at 11–12; Ex. 1006 ¶ 44 (Cryptograph means 590 includes means to perform a digital signature and “is used to establish secured communication,” and further to “handl[e] digital signatures and certificates”); Ex. 1001, 3:44–45 (“The security-establishing operation will be the signing of an electronic document.”); Ex. 1003 ¶ 81. In other words, Cheng reasonably teaches that its cryptograph means is used specifically to handle digital signatures in addition to establish secured communications. Ex. 1006 ¶ 44. Contrary to Patent Owner’s contentions, the well-known security-establishing operation of performing a digital signature taught by Cheng would have been directed to the security of the transaction and would have been “within” the transaction as claimed because it would have authenticated data or a document corresponding to the transaction. Ex. 1026 ¶¶ 6, 9, 13–15, 17; Ex. 1008, 2:5–10, 2:16–30, 21:38–43, Fig. 75; Ex. 1027, 1:25–38; Ex. 1029, 617.

Furthermore, we are unpersuaded by Patent Owner’s arguments attempting to distinguish the claim over a narrowing claim interpretation lens that we have rejected in our claim construction analysis. *See supra* Section VIII. For instance, we repeat here that the claim language may encompass operations that establish security by further encrypting the communication of the transaction document. Petitioner has persuasively shown that Cheng’s cryptograph means are used to establish the secured communication and to handle digital signatures, and that a person of ordinary skill in the art had the knowledge on how to secure a smart card transaction using well known encryption operations. Ex. 1003 ¶¶ 81–82; Ex. 1026 ¶¶ 6, 9, 13–15, 17. Thus, Petitioner has shown that digital signatures were used to secure transactions via smart card and that the

communications during the transaction were encrypted. This is sufficient to show by a preponderance of the evidence that the combination of Burger and Cheng teaches or suggests “the portable data carrier then performs a security establishing operation within the electronic transaction.” We further credit the testimony of Dr. Neuman in finding that signing the electronic transaction of Burger using the digital signature operation of Cheng teaches “the portable data carrier then performs a security establishing operation within the electronic transaction” as claimed.

1.4 creating authentication quality information

Claim 1 recites “comprising the steps of creating authentication quality information by the portable data carrier about said user authentication method used.” Claim 10 recites “wherein the data carrier is arranged to create quality information about said user authentication method used.” Petitioner contends that the combination of Burger and Cheng teaches these limitations of claims 1 and 10. Pet. 49–51, 66. Petitioner contends that Burger discloses a Pocket Vault that performs various types of user authentication methods of differing quality, and authenticates a user using one of the authentication methods prior to a transaction. *Id.* at 49 (citing Ex. 1005, 12:6–27, 16:28–55, 22:66–23:19). Petitioner contends that, to the extent Burger does not explicitly disclose creating information about the quality of the method used, Cheng discloses creating and storing information representing the authentication level and method used. *Id.* at 49–50 (citing Ex. 1006 ¶¶ 10, 33–34, 43, 45, table 1).

Patent Owner does not dispute Petitioner’s contentions. We find that the combination of Burger and Cheng teaches these limitations of claims 1 and 10.

1.5 attaching said quality information to the result

Claim 1 recites “attaching said authentication quality information to the result of the security-establishing operation.” Claim 10 recites “to attach such quality information to the result of the security establishing operation.”

Petitioner contends that Cheng discloses these limitations of claims 1 and 10 in creating an electronic identifier representing the authentication level of the authentication method used, and securely communicating the electronic identifier to the authorizer device by performing a digital signature. Pet. 51–52 (citing Ex. 1006 ¶¶ 31, 36, 44, 45), 66. Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that Cheng discloses the features recited in these limitations of claims 1 and 10.

Patent Owner contends that a person of ordinary skill would not have combined a digital signature with the secure communications between devices as taught by Burger to yield this limitation. PO Sur-Reply 17–18. Patent Owner contends that, by using a digital signature for communication, the original information will be publicly transmitted, which would be detrimental, because the information could be high security information such as an electronic version of a credit card. *Id.* at 19–21. Patent Owner contends that a person of ordinary skill would not be motivated to modify Burger’s encrypted communication system to implement Cheng’s digital signature process because the modification would destroy the basic objective of the prior art. *Id.* at 21.

We agree with Patent Owner, that in “conventional digital signature techniques . . . the [original] message M is made public with the digital signature A attached to it.” PO Sur-Reply 20 (citing Ex. 1026 ¶ 13; Ex. 1027, 1:25–30). We note that Patent Owner’s contention contradicts

Patent Owner's earlier contention that the digital signature of the '249 Patent is "within" a transaction, because the digital signature of the '249 Patent could be transferred without employing an encrypted communication system. *Id.* at 10–12. We agree that a conventional digitally signed message, such as a message taught by the combination of Burger and Cheng, could be transferred without being encrypted, because the purpose of the digital signature is authentication rather than secrecy. Ex. 1029, 617; Ex. 1008, 2:5–10; Ex. 1026 ¶ 6. Further, the digitally signed message can be encrypted to provide secrecy. Ex. 1026 ¶¶ 8–9; Ex. 1006 ¶¶ 44, 46; Ex. 1007 ¶¶ 49–50, 52, 57; Ex. 1008, 10:47–55, 22:24–36. We find that a person of ordinary skill, after performing a security-establishing operation and attaching authentication quality information to the result of the security-establishing operation as taught by the combination of Burger and Cheng, would have encrypted the communications sent from Burger's Pocket Vault to yield the benefit of preventing any attacker who intercepts those communications from receiving useful information as taught by Burger. Ex. 1005, 55:23–36.

Patent Owner contends that the electronic identifier of Cheng, which represents the authentication quality information, would be an input to the digital signature process, and therefore, could not be "attached to the result of the security establishing operation" as claimed. PO Resp. 17–19. According to Patent Owner, the digital signature by itself would be communicated to the receiving device, without the electronic identifier attached to it. *Id.*

Petitioner contends that a digital signature is meant to be attached to the original document from which it is created, because it has no utility on its own. Pet. Reply 14 (citing Ex. 1027, 1:25–30). Petitioner contends that

the purpose of a digital signature is to allow the recipient to authenticate a document, and therefore requires both the document and the digital signature, because the original document cannot be derived from the digital signature. *Id.* (citing Ex. 1026 ¶¶ 6, 9, 10). Petitioner contends that when the Pocket Vault of Burger communicates the authentication level information, it would attach it to the digital signature, as was conventional. *Id.* at 14–18 (citing Pet. 51–53; Ex. 1003 ¶¶ 88–91; Ex. 1007 ¶¶ 51, 53, Fig. 1; Ex. 1008, 21:17–42, Fig. 75; Ex. 1026 ¶¶ 6–11).

Patent Owner contends that Cheng teaches that the authorizer selects an access authentication level from different authentication levels. PO Sur-Reply 14–15 (citing Ex. 1006 ¶¶ 10, 11, 37, 39, 45). This means that, according to Patent Owner, the authentication level information is known a priori to the authorizer. *Id.* at 15. Patent Owner contends that, because the particular authorization level must be known to the authorizer, the digital signature sent to the authorizer need not contain an accompanying message with the electronic identifier of the authorization level. *Id.* at 15–17 (citing Ex. 1026, 5; Ex. 2014, 45:4-46:19).

Patent Owner’s contention, that the authorizer would know the particular authorization level, is inconsistent with the teachings of Cheng. Cheng discloses that an “electronic identifier represents a unique identification of the access authentication level and authentication factors entered by the authorizee.” Ex. 1006 ¶ 45. Cheng discloses that “[g]reater flexibility is provided to an authorizee in allowing modifications to an authentication level and/or authentication factors.” *Id.*, Abstract; *see also id.* ¶¶ 7–8 (describing that the authorizee also has flexibility to select alternative authentication factors and to modify the authentication level selected from a list). Cheng discloses that “[t]his would allow an authorizee for instance to

select an alternative authentication factor in case the authorizee is not able to communicate the intended authentication factor.” *Id.* ¶ 38. Cheng gives, as an example, that when the requested authentication factor is a thumbprint, and the authorizee had a cut from a knife in that thumb, the authorizee would select an alternative authentication factor. *Id.* Because the authorizer would not know whether the authorizee changed the authentication level or the authentication factors unless the authorizee informed the authorizer, we disagree with Patent Owner’s contention that the authentication quality information of Cheng would not need to be attached to the digital signature. *See* Ex. 1003 ¶ 88; Ex. 1006 ¶¶ 31, 36, 45 (“In some cases, it might be necessary to communicate the authentication level, and thus the authentication factor(s), through an electronic identifier.”).

We agree with Petitioner, that a person of ordinary skill would have attached the electronic identifier to the digital signature of Cheng for transmission by Burger’s Pocket Vault to the point-of-sale terminal for the benefit of allowing the recipient to authenticate the identifier, as was conventional. *Pet.* 51-53; *Pet. Reply* 18; Ex. 1003 ¶¶ 88–91; Ex. 1026 ¶¶ 6-17. For example, Russo describes attaching seal 130 containing a digital signature of envelope 120 to the envelope, where the envelope contains authentication quality information in the form of authentication trust metric 190. *Ex. 1007*, Fig. 1, ¶¶ 51, 53. As another example, Wheeler describes that “the digital signature . . . typically is appended to the message.” *Ex. 1008*, 1:60–62; *see id.* at Fig. 75 (Showing authentication information (EAI) and message M2 attached to a digital signature of the message DS(M2)), 21:17-45. We credit the testimony of Dr. Neuman in determining that the combination of Burger and Cheng teaches these limitations of claims 1 and 10.

1.6 wherein the difference in quality . . .

Claims 1 and 10 each recite “wherein the difference in quality of said user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective.” Petitioner contends that the combination of Burger and Cheng teaches these limitations of claims 1 and 10. Pet. 53–55, 65. Petitioner contends that Burger teaches that the Pocket Vault performs various methods of authentication, such as PIN-based or biometric-based. *Id.* at 53–54 (citing Ex. 1005, 12:6–16). Petitioner contends that Cheng teaches that a biometric-based authentication method has a higher authentication level, or quality, than a PIN-based method. *Id.* at 54 (citing Ex. 1006 ¶¶ 33–34, table 1). Patent Owner does not dispute Petitioner’s contentions. We find that the combination of Burger and Cheng teaches these limitations of claims 1 and 10.

Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined teachings would have taught or suggested the features recited in claims 1 and 10 to an ordinarily skilled artisan.

5. Claims 2 and 11

Claim 2 depends from claim 1 and recites “wherein the security establishing operation performed by the portable data carrier comprises creating a digital signature.” Claim 11 depends from claim 2 and recites “wherein the portable data carrier is set up to create a digital signature.” Petitioner contends that the combination of Burger and Cheng teaches these limitations of claims 2 and 11. Pet. 55–56, 66. Petitioner contends that

Burger teaches a Pocket Vault that performs well known security establishing operations, such as PKI-based operations, to secure its communications. *Id.* at 55 (citing Ex. 1005, 12:37–51; 55:29–35).

Petitioner contends that Cheng teaches that one well known security establishing operation is creating a digital signature. *Id.* (citing Ex. 1006 ¶ 44). Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claims 2 and 11.

6. Claim 3

Claim 3 depends from claim 1 and recites “wherein the authentication of the user is performed by presentation of a biometric feature.” Petitioner contends that Burger discloses this limitation in describing authenticating a user by scanning the user’s fingerprint. Pet. 56 (citing Ex. 1005, 12:6–27, 22:36–52, 23:1–4). Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 3.

7. Claim 4

Claim 4 depends from claim 3 and recites “wherein the authentication of a user is performed by presentation of a physiological or behavior-based feature characteristic of a user.” Petitioner contends that Burger discloses this limitation in describing authentication by scanning a physiological feature such as a fingerprint, an iris, a retina, or a voiceprint. Pet. 57 (citing Ex. 1005, 22:36–52, 23:1–4, 17:50–67). Petitioner contends that Burger discloses authentication by analyzing behavior-based features such as a speech pattern analysis or keystroke rhythm. *Id.* (citing Ex. 1005, 12:6–27).

Patent Owner does not dispute Petitioner's contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 4.

8. *Claim 5*

Claim 5 depends from claim 1 and recites "wherein the authentication of the user is performed by proof of knowledge of a secret." Petitioner contends that Burger discloses this limitation in describing a PIN code that may be entered by the holder to verify the holder's identity. Pet. 57 (citing Ex. 1005, 12:16–27). Patent Owner does not dispute Petitioner's contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 5.

9. *Claims 6 and 12*

Claim 6 depends from claim 1 and recites "wherein at least two different authentication methods of different quality are offered for authentication of the user." Claim 12 depends from claim 10 and recites "wherein the data carrier supports at least two qualitatively different authentication methods." Petitioner contends that the combination of Burger and Cheng teaches these limitations of claims 6 and 12. Pet. 58–59, 67. Petitioner contends that Burger discloses a Pocket Vault that offers multiple, alternative authentication methods of different quality, such as biometric-based and PIN-based authentication methods. *Id.* at 58 (citing Ex. 1005, 12:6–27). Petitioner contends that Cheng discloses a portable authentication device that permits a user to select one or more authentication factors from a plurality of authentication factors, such as biometric factors and non-biometric factors. *Id.* at 58–59 (citing Ex. 1006 ¶ 38). Petitioner contends

that Cheng teaches that a benefit of allowing a user to select from different authentication methods of different quality is that the user can select an alternative authentication factor in case the user is not able to communicate with the intended authentication factor. *Id.* Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claims 6 and 12.

10. Claim 7

Claim 7 depends from claim 6 and recites “wherein the particular authentication methods not used are disabled.” Petitioner contends that the combination of Burger and Cheng teaches this limitation. Pet. 60–61. Petitioner contends that Burger discloses a Pocket Vault that offers authentication methods “alternatively,” such that when one of the several methods is used for authentication, the methods not used are not available for communication, and are therefore disabled. *Id.* at 60 (citing Ex. 1003, Neuman Decl. ¶¶ 104–105). Petitioner also contends that Cheng discloses that a user has the ability to delete an authentication factor, such as a fingerprint factor, and that in such a case, the fingerprint scanner located on the portable device would be disabled for authentication. *Id.* (citing Ex. 1006 ¶¶ 7–8; Ex. 1003, Neuman Decl. ¶¶ 106–108). Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 7.

11. Claim 8

Claim 8 depends from claim 6 and recites “wherein no quality information is produced for an authentication method.” Petitioner contends that Cheng discloses this limitation in describing creating information about

the authentication level and authentication factors entered by the user, and does not create authentication level information for authentication factors not entered by the user. Pet. 61–63 (citing Ex. 1006 ¶ 45; Ex. 1003, Neuman Decl. ¶ 109). Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 8.

12. Claim 9

Claim 9 depends from claim 1 and recites “wherein a user is asked to select an authentication method.” Petitioner contends that the combination of Burger and Cheng teaches this limitation. Pet. 63–65. Petitioner contends that Burger discloses a touch-screen enabled Pocket Vault that performs multiple user authentication methods of different quality, where the methods are offered alternatively or additionally. *Id.* (citing Ex. 1005, 12:6–27, 22:12–16). Petitioner contends that Cheng teaches allowing a user to select an authentication method via a display on a portable authentication device. *Id.* (citing Ex. 1006 ¶¶ 8, 38, 41). Petitioner contends that causing Burger’s Pocket Vault to ask a user on its touch screen to select an authentication method yields the predictable benefit of providing flexibility to the user as taught by Cheng. *Id.* at 64 (citing Ex. 1003, Neuman Decl. ¶ 115). Patent Owner does not dispute Petitioner’s contentions. We find that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng and that their combined disclosures teach the limitations recited in claim 9.

X. CONCLUSION⁵

Claims 1–12 are unpatentable over the prior art.

Claim(s)	35 U.S.C. §	Reference(s)/Basis	Claims Shown Unpatentable	Claims Not shown Unpatentable
1–12	103	Burger, Cheng	1–12	
Overall Outcome			1–12	

XI. ORDER

It is hereby:

ORDERED claims 1–12 are unpatentable; and

FURTHER ORDERED that because this is a final written decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.

⁵ Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. See 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. See 37 C.F.R. § 42.8(a)(3), (b)(2).

IPR2022-01135
Patent 8,205,249 B2
FOR PETITIONER:

Scott T. Jarratt
Andrew S. Ehmke
Calmann J. Clements
HAYNES AND BOONE, LLP
scott.jarratt.ipr@haynesboone.com
andy.ehmke.ipr@haynesboone.com
calmann.clements.ipr@haynesboone.com

FOR PATENT OWNER:

Brett Cooper
BC LAW GROUP, P.C.
bcooper@bc-lawgroup.com

Robert A. Auchter
AUCHTER PLLC
robert@auchterlaw.com