

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

AIRE TECHNOLOGY LIMITED,
Patent Owner.

IPR2023-00080
Patent 8,205,249 B2

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

SMITH, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Petitioner, Apple Inc., filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claim 13 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 Preliminary Response (Paper 6, “Prelim. Resp.”) pursuant to 35 U.S.C. § 313.

Pursuant to 35 U.S.C. § 314(a), the Director may not authorize an *inter partes* review unless the information in the petition and preliminary response “shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” For the reasons that follow, we institute an *inter partes* review as to claim 13 of the ’249 patent on the ground of unpatentability asserted in the Petition.

II. REAL PARTIES-IN-INTEREST

Petitioner identifies itself (Apple, Inc.) as its sole real party-in-interest. Pet. 69. Patent Owner identifies itself (Aire Technology Ltd.) as its sole real party-in-interest. Paper 3, 2.

III. RELATED MATTERS

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

Aire Technology Ltd. v. Samsung Electronics Co., Ltd. et al., No. 6-21-00955 W. D. Tex., filed Sep. 15, 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. Google LLC, No. 6-21-01104, W.D. Tex., filed Oct. 25, 2021;

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

Apple, Inc. v. Aire Technology Ltd., IPR2022-01135 (PTAB, June 15,
2022).

Pet. 69. Patent Owner identifies the following additional proceedings as
“related current and/or former proceedings involving the patent-at-issue.”

Paper 3, 2.

Apple Inc. v. Aire Technology Ltd., IPR2022-01135 (PTAB June 15,
2022);

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

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 is shown below

Fig. 1

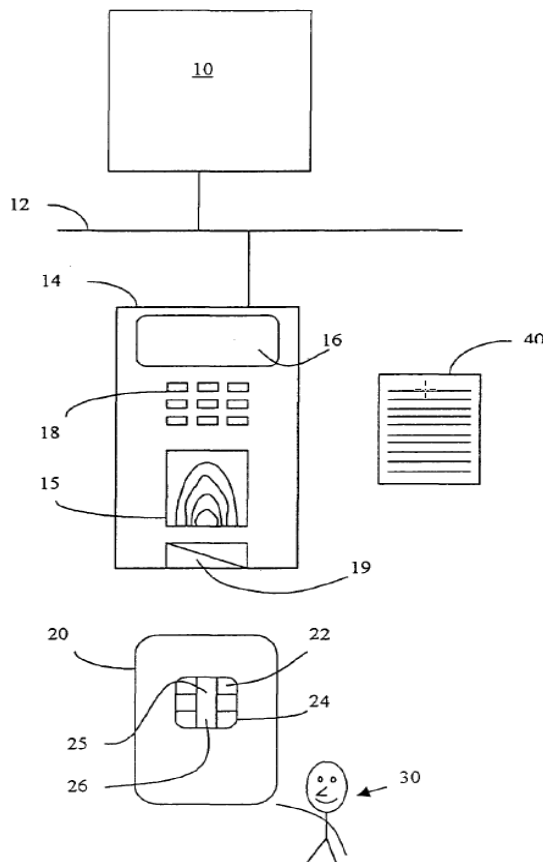


Figure 1 above illustrates a structure of a transaction system for effecting a secure electronic transaction. Ex. 1001, 3:17–18. Data network 12 exchanges data between terminal 14 and background system 10. *Id.* at 3:42–43. Terminal 14 includes display screen 16 and input means 18. *Id.* at 3:46–49. 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 3:57–61.

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 3:29–33.

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 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 13 of the ’249 patent recites:

13. A terminal for use in connection with a portable data carrier, said terminal including a device arranged to cause a user to select one of at least two possible different quality authentication methods, wherein the portable data carrier is arranged to perform a user authentication using one of the at least two possible different quality authentication methods and to confirm the authentication to the terminal, and the data carrier is arranged to create quality information about the authentication

method used and to attach such quality information to the result of a security establishing operation, the difference in quality of said 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 claim 13 of the '249 patent are unpatentable on the following ground.

Claim(s) Challenged	35 U.S.C. § ¹	Reference(s)/Basis
13	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 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*, Prelim. 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

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).

(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, “although claim 13 is not at issue in parallel 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. 14. In the district court, Patent Owner asserted no construction is necessary. *Id.* at 15. Petitioner adopts Patent Owner’s district court proposed construction for purposes of this proceeding. *Id.*

For purposes of this Decision, 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. See Section IX *infra*.

Claim 13 recites “the data carrier is arranged to create quality information about the authentication method used and to attach such quality information to the result of a security establishing operation.” Patent Owner contends that “claim 13 requires the performance of a ‘security establishing operation’ and that a portable data carrier (i) ‘*create quality information about the authentication method used*’; and (ii) ‘***such quality information [is attached] to the result of [the] security establishing operation.***’” Prelim. Resp. 9–10. Patent Owner contends that even though the claim does not recite performing a security establishing operation, the claim requires performing the security establishing operation, otherwise, there would not be a “result of a security establishing operation” as claimed. *Id.* at 10. 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 claim requires attaching the quality information to the claimed “result” of the operation. *Id.* at 11.

For purposes of this Decision, we construe “the data carrier is arranged to create quality information about the authentication method used and to attach such quality information to the result of a security establishing operation” to encompass at least attaching quality information to an encrypted document, such as a digitally signed document. We further construe the claimed “quality information” that is “attach[ed]” to “the result” to encompass digitally signed quality information. That is, the claim does not require the attached quality information to be unsigned. Further, we agree with Patent Owner, that “an exemplary ‘security establishing operation’ [is] creating a digital signature” (Prelim. Resp. 10), and therefore is not limited to an operation that creates a digital signature. We construe the claimed “security establishing operation” to encompass the example of creating a digital signature, and does not exclude other operations that establish security, such as encryption operations generally. Should the parties disagree with this construction, the parties are invited to address this issue further.

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 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

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

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. Claim 13 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 bio-metric 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

Table 1, above, provides an example of different authentication levels and associated authentication methods, such as associating authentication factors of “Possession” for “Authentication Level 1.” 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 Cheng because both references concern methods for effecting secure electronic transactions with a portable authentication device, and the combination provides the benefit of allowing 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. 37–47 (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. 45–47 (citing Ex. 1003, Neuman Decl. ¶ 61).

For purposes of this Decision, we find Petitioner cites sufficient evidence to support its contention that a person of ordinary skill would have had reason to combine the teachings of Burger and Cheng.

4. Claim 13

The preamble of claim 13 recites a “terminal for use in connection with a portable data carrier.” Petitioner contends that Burger teaches a terminal for use in connection with a portable data carrier in disclosing a point-of-sale terminal used in connection with an individual’s hand-held portable electronic authorization device, referred to as a Pocket Vault. Pet. 47–48. Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that Burger and Cheng teach the features recited in the preambles of claim 13.

Claim 13 recites “said terminal including a device arranged to cause a user to select one of at least two possible different quality authentication methods.” Petitioner contends that the combination of Burger and Cheng teaches this limitation. Pet. 47–55. Petitioner contends that the Pocket Vault of Burger authenticates a user using a personal identification number (PIN) code or a fingerprint scanner before approving a transaction request. Pet. 48–49. Petitioner contends that Burger teaches that the operator of the terminal can select an option to require authentication. Pet. 50–52. Petitioner contends that Cheng teaches that a user of an authentication

device can select an authentication factor from a plurality of authentication factors. Pet. 52–54. Petitioner contends that when the operator of Burger’s terminal selects an option to require authentication, a person of ordinary skill would have found it obvious for the Pocket Vault to prompt a user to select between different quality authentication methods as taught by Cheng. Pet. 54–55. Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that the combination of Burger and Cheng teaches the features recited in this limitation of claim 13.

Claim 13 recites “wherein the portable data carrier is arranged to perform a user authentication using one of the at least two possible different quality authentication methods and to confirm the authentication to the terminal.” Petitioner contends that Burger teaches this limitation in disclosing scanning a fingerprint, determining whether the fingerprint matches a stored fingerprint, and if so, confirming the result to the terminal. Pet. 55–57. Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that the combination of Burger and Cheng teaches the features recited in this limitation of claim 13.

Claim 13 recites “the data carrier is arranged to create quality information about the authentication method used.” Petitioner contends that the combination of Burger and Cheng teaches this limitation. Pet. 57–60. Petitioner contends that Burger teaches that various authentication methods have varying security levels, and that Cheng teaches assigning authentication levels to different authentication methods, or factors. Pet. 57–60. Based on the evidence and arguments currently of record, for purposes of institution, we find that Petitioner has demonstrated that the combination

of Burger and Cheng teaches the features recited in this limitation of claim 13.

Claim 13 recites “to attach such quality information to the result of a security establishing operation.” Petitioner contends that the combination of Burger and Cheng teaches this limitation. Pet. 60–66. Petitioner contends that Burger teaches that communications between the Pocket Vault and the terminal are secured by known security establishing operations, such as public or private key encryption techniques. Pet. 60–63. Petitioner contends that Cheng teaches that one known security establishing operation is a digital signature. Pet. 63. Petitioner contends that Cheng teaches that all communications may be secured by performing a digital signature. Pet. 64. Petitioner contends that it would have been obvious to attach the authentication level information to a digital signature of the transaction. Pet. 65–66 (citing Ex. 1003 ¶ 100; Ex. 1007 ¶¶ 51, 53, Fig. 1 (describing attaching an “Authentication Trust Metric” to the “digital signature . . . signed in a preferred embodiment with the private key of the authenticating party” for transmission); Ex. 1008, 21:17-42, Fig. 75 (describing attaching an “Entity Authentication indicator (EAI)” to a “digital signature” for transmission from an account holder to an account authority)).

Patent Owner’s Argument about the “security establishing operation”

Patent Owner contends that neither Burger nor Cheng teaches the claimed “security establishing operation.” Prelim. Resp. 11–15. According to Patent Owner, the ’249 patent describes the “security establishing operation” as the signing of an electronic document, which is separate and distinct from securing communications using encryption operations. Prelim. Resp. 11–13. According to Patent Owner, the “‘security-establishing operation’ of the ’249 patent is directed to the security of the *transaction*,

not the security of the *communication* between the parties in the transaction.” *Id.* at 11. Patent Owner contends that Burger and Cheng teach secure, encrypted communications, but do not perform the security establishing operation for a security-critical transaction, such as the placing of service orders involving costs. *Id.* at 12–13. Patent Owner contends that Cheng uses the digital signature to establish secured communications between devices, but does not teach a “security establishing operation” as claimed. Prelim. Resp. 14.

Patent Owner’s distinction between securing all communications using one type of encryption operation, and further securing a security-critical transaction with a second “security establishing operation,” is not recited in claim 13. Patent Owner’s contention is not commensurate with the scope of the claim.

On this record, we agree with Petitioner that Burger performs known PKI-based security establishing operations. Pet. 63. We also agree with Petitioner, that one known PKI-based security establishing operation is the performance of a digital signature as taught by Cheng. *Id.* Cheng discloses a cryptographic means “includ[ing] means to perform . . . a digital signature” for the benefits of “establish[ing] secured communication between” devices and “cipher[ing] cryptic communication to/from [an] authorizer.” Ex. 1006 ¶ 44. Petitioner’s declarant, Dr. Neuman, testifies that “Cheng further teaches that all communications, such as the communication of the electronic identifier representing authentication level information, may be secured by performing a digital signature.” Ex. 1003 ¶ 99. Dr. Neuman testifies that it would have been obvious for the Pocket Vault of Burger to perform a digital signature to secure communications because doing so was

well known and routine in the art. Ex. 1003 ¶ 97 (citing Ex. 1010, 9:54-10:4; Ex. 1007 ¶ 24; Ex. 1011, 1:6-31, 2:1-14, 4:16-22).

On this record, we agree with Petitioner, that it would have been obvious to use the digital signature of Cheng when performing the PKI-based security operation of Burger. Pet. 63. We rely on the testimony of Dr. Neuman in determining, on this record, that using the digital signature operation of Cheng to secure the transaction information of Burger does no more than yield the predictable result of securing the transaction information of Burger, as was well-known in the art. *See* Ex. 1003 ¶ 97 (citing Ex. 1007 ¶ 24; Ex. 1011, 1:6–31, 2:1–14, 4:16–22); *KSR*, 550 U.S. at 421 (“[A] person of ordinary skill has good reason to pursue the known options within his or her technical grasp.”); *see id.* at 416 (“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.”).

Patent Owner’s Argument about attaching information to the result

Patent Owner contends that neither Burger nor Cheng teaches attaching the quality information to the result of the security establishing operation. Prelim. Resp. 15–19. According to Patent Owner, Cheng teaches securing communication through a digital signature. *Id.* at 17. Patent Owner contends that Burger, when modified to encrypt Cheng’s quality information using the digital signature operation of Cheng, would produce a digital signature of the quality information, but would not produce quality information attached to a digital signature. *Id.* at 18.

However, as discussed above in our claim construction, claim 13 does not require the quality information to be unsigned. Even were we to accept the premise of Patent Owner’s argument, that all communications sent from Burger’s device, including the transaction information and the quality

information, would be secured using the digital signature operation of Cheng, we are sufficiently persuaded that attaching the digitally signed quality information of Cheng to the digitally signed transaction of Burger teaches attaching quality information to the result of a security establishing operation within the scope of claim 13. *See* Pet. 64–65.

Further, Patent Owner’s contention does not address Petitioner’s combination, that attaching the quality information to the digitally signed transaction would have been predictable and likely to succeed because the prior art literature was replete with examples of systems that similarly attached authentication quality information to a digital signature for transmission. Pet. 64–65. Dr. Neuman testifies that the prior art literature includes many examples of systems that attach authentication quality information to a digital signature of a transaction. Ex. 1003 ¶ 100. Dr. Neuman, citing Figure 1 of Russo (Ex. 1007), testifies that Russo teaches attaching quality information (authentication trust metric 190) to a digital signature signed with a private key of the authenticating party (seal 130). Ex. 1003 ¶ 100. Dr. Neuman, citing Figure 75 of Wheeler (Ex. 1008), testifies that Wheeler teaches attaching an entity authentication indicator to a digital signature for a message for transmission from an account holder to an account authority. Ex. 1003 ¶ 100.

On this record, we are persuaded by Dr. Neuman’s testimony, that the transaction and corresponding quality information would have been attached to the digital signature before sending the digital signature, transaction, and quality information from the device as taught by the prior art. *See* Ex. 1003 ¶ 100 (citing Ex. 1007, Fig. 1; Ex. 1008, Fig. 75). For example, Wheeler discloses that a “digital signature is used to ‘authenticate’ a message.” *Id.* at 2:8–9. Wheeler discloses that creating a digital signature includes

calculating a message digest such as a hash value, and encrypting the message digest. Ex. 1008, 1:54–57. Wheeler discloses that the “resulting cyphertext itself usually constitutes the digital signature, *which typically is appended to the message.*” *Id.* at 1:60–62. Figure 75 of Wheeler shows an electronic communication (EC) that includes a message (M2), a digital signature of the message (DS(M2)), and an entity authentication indicator (EAI). Ex. 1008, 21:17–43, Fig. 75. As another example, Figure 1 of Russo shows transaction 140 and authentication trust metric 190 attached to envelope 120, which includes seal 130 containing a digital signature. Ex. 1007 ¶¶ 46, 51, 53, Fig. 1. Thus, Russo and Wheeler each show “authentication quality information” that is “attach[ed]” to a digital signature, or “result of the security-establishing operation” as claimed.

Further, we agree with Petitioner, that Cheng teaches attaching the quality information through an electronic identifier. *See* Pet. 63–64 (citing Ex. 1007 ¶¶ 31, 36, 44–45). Cheng teaches communicating the access authentication level through an electronic identifier, such as a public-key certificate. Ex. 1006 ¶ 45. Cheng teaches that an originator encrypts a confidential message and sends the encrypted document to a recipient. *Id.* at ¶ 46. As discussed above, Cheng teaches digitally signing the encrypted document. Ex. 1006 ¶ 44. Cheng teaches that the recipient receives the encrypted document and “analyzes the *attached public-key certificate*” to authenticate itself “in accordance with *the access authentication level indicated in the certificate.*” *Id.* at ¶ 46.

On this record, we are persuaded by Dr. Neuman’s testimony and the knowledge of a person of ordinary skill as shown by Cheng (and supported by Dr. Neuman’s discussion of Russo and Wheeler) that attaching the

authentication level information to the digital signature of Burger's transaction would have been obvious.

Claim 13 recites "the difference in quality of said 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 this limitation. Pet. 66–67. Petitioner contends that Burger teaches performing different types of user authentication methods of varying quality, such as PIN-based methods and fingerprint-based methods. Pet. 66. Petitioner contends that Cheng teaches that the fingerprint-based method has a higher quality than the PIN-code method. Pet. 66.

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 claim 13 to an ordinarily skilled artisan.

X. CONCLUSION

Based on the arguments presented in the Petition, we conclude that Petitioner has demonstrated a reasonable likelihood of prevailing with respect to claim 13 of the '249 patent challenged in the Petition. Accordingly, we institute a trial on the claim and the ground asserted in the Petition. The Board has not made a final determination under 35 U.S.C. § 318(a) with respect to the patentability of the challenged claim.

XI. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claim 13 of the '249 patent is instituted with respect to the ground set forth in the Petition; and

FURTHER ORDERED that, pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4(b), *inter partes* review of the '249 patent shall commence on the entry date of this Decision, and notice is hereby given of the institution of a trial.

IPR2023-00080
Patent 8,205,249 B2

FOR PETITIONER:

Scott Jarratt
Andrew Ehmke
Calmann Clements
HAYNES & 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 Auchter
AUCHTER PLLC
robert@auchterlaw.com