Trials@uspto.gov
571-272-7822

PUBLIC VERSION

Paper No. 54
Entered: May 1, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, INC.,
Petitioner,

v.

UNIVERSAL SECURE REGISTRY LLC,
Patent Owner.

Case IPR2018-00067
Patent 8,577,813 B2

Before BART A. GERSTENBLITH, SCOTT C. MOORE, and JASON W. MELVIN, *Administrative Patent Judges*.

MELVIN, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Petitioner, Unified Patents Inc., requested *inter partes* review of claims 1–3 and 5–26 of U.S. Patent No. 8,577,813 B2 (Ex. 1001, "the '813 patent"). Paper 12 ("Pet.").[1] Patent Owner, Universal Secure Registry LLC, filed a Preliminary Response (Paper 7, "Prelim. Resp.") and a Supplemental Preliminary Response (Paper 13, "Supp. Prelim. Resp.").[2] We instituted review. Paper 14 ("Inst." or "Institution Decision"). Patent Owner filed a Response (Paper 28 ("PO Resp.")) and a Conditional Motion to Amend (Paper 26 ("MTA")); Petitioner filed a Reply (Paper 39 ("Reply")) and an Opposition to Patent Owner's Contingent Motion to Amend (Paper 34 ("MTA Opp.")); Patent Owner filed a Surreply (Paper 42) and a Reply to Petitioner's Opposition (Paper 43 ("MTA Reply")); and Petitioner filed a Surreply to the Contingent Motion to Amend (Paper 44 ("MTA Surreply")). We held a hearing on January 30, 2019, and a transcript is included in the record. Paper 51 ("Tr.").

This is a final written decision as to the patentability of the challenged claims. For the reasons discussed below, we determine that Petitioner has proven by a preponderance of the evidence that each of claims 1–3, 5–9, 11, 13–18, 20, and 22–26 of the '813 patent is unpatentable but has not proven that any of claims 10, 12, 19, and 21 is unpatentable. We deny Patent Owner's Contingent Motion to Amend.

[1] We authorized Petitioner to file a Corrected Petition. *See* Paper 11.
[2] We authorized Patent Owner to file a Supplemental Preliminary Response addressing claims 7–10. Paper 11, 5–7.

A. RELATED MATTERS

The parties identify the following judicial matter involving the '813 patent: *Universal Secure Registry LLC v. Apple Inc. et al.*, Case No. 1:17-cv-00585 (D. Del.) (filed May 21, 2017). Pet. 67; Paper 5.

B. THE '813 PATENT

The '813 patent issued November 5, 2013, from an application filed September 20, 2011. Ex. 1001, [45], [22]. The '813 patent includes a number of priority claims, including dates as early as February 21, 2006. *Id.* at [63], [60], 1:6–32.

The '813 patent is titled "Universal Secure Registry" and is directed to authenticating a user using biometric and secret information provided to a user device, encrypted, and sent to a secure registry for validation. *Id.* at Abstract. The Specification describes one aspect of the invention as an "information system that may be used as a universal identification system and/or used to selectively provide information about a person to authorized users." *Id.* at 3:65–4:1. One method described for controlling access involves "acts of receiving authentication information from an entity at a secure computer network, communicating the authentication information to the secure registry system, and validating the authentication information at the secure registry system." *Id.* at 4:43–48. The "universal secure registry" ("USR") is described as a computer system with a database containing entries related to multiple people, with a variety of possible information about each person, including validation, access, and financial information. *Id.* at 9:35–12:18.

Validation information in the '813 patent "is information about the user of the database to whom the data pertains and is to be used by the USR software 18 to validate that the person attempting to access the information is the person to whom the data pertains or is otherwise authorized to receive it." *Id.* at 12:19–23. Such information must "reliably authenticate the identity of the individual" and may include "a secret known by the user (e.g., a pin, a phrase, a password, etc.), a token possessed by the user that is difficult to counterfeit (e.g., a secure discrete microchip), and/or a measurement such as a biometric (e.g., a voiceprint, a fingerprint, DNA, a retinal image, a photograph, etc.)." *Id.* at 12:23–31. The '813 patent describes using such information in combination with other information "to generate a one-time nonpredictable code which is transmitted to the computer system" and used "to determine if the user is authorized access to the USR database." *Id.* at 12:50–60; *see also id.* at 45:55–46:36. Communication between a user device and the secure registry may occur through a point-of-sale ("POS") device in the '813 patent. *Id.* at 43:4–44:31.

C. CHALLENGED CLAIMS

Petitioner challenges claims 1–3 and 5–26. Challenged claims 1, 16, and 24 are independent. Claim 1 (reproduced below) is illustrative of the claimed subject matter:

> 1[P]. An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> [a] a biometric sensor configured to receive a biometric input provided by the user;
>
> [b] a user interface configured to receive a user input including secret information known to the user and

identifying information concerning an account selected by the user from the plurality of accounts;

[c] a communication interface configured to communicate with a secure registry;

[d] a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface,

[i] the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information,

[ii] the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information, and

[iii] to communicate the encrypted authentication information via the communication interface to the secure registry; and

[e][i] wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and

[ii] wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

Ex. 1001, 51:65–52:29.[3]

[3] We include square-bracketed annotations following Petitioner's demarcations. *See* Pet. 9–26.

D. GROUNDS OF UNPATENTABILITY

Petitioner asserts the following grounds of unpatentability, each based on 35 U.S.C. § 103(a):[4]

References	Challenged Claim(s)
Maes[5] and Pare[6]	1–3, 5, 11, 13–17, 20, and 22–26
Maes and Labrou[7]	1–3, 5, 11–17, and 19–26
Maes, Pare, and Labrou	12–15, 17, 19–23, 25, and 26
Maes, Pare, and Burger[8]	6–9 and 18
Maes, Labrou, and Burger	6–10 and 18
Maes, Pare, Burger, and Labrou	10
Pizarro[9] and Pare	1, 2, 5, 11, 13, 16, 17, and 24

See Pet. 4–5; Inst. 30–31. Petitioner also relies on the Declaration of Dr. Eric Cole (Ex. 1009) and Declaration of Dr. Eric Cole in Support of Petitioner's Reply to Patent Owner's Response (Ex. 1032), while Patent Owner relies on the Declaration of Markus Jakobsson in Support of Patent Owner's Response (Ex. 2004).

[4] The America Invents Act includes revisions to, *inter alia*, 35 U.S.C. § 103 effective on March 16, 2013. Because the '813 patent issued from an application filed before March 16, 2013, the pre-AIA version of 35 U.S.C. § 103 applies.
[5] U.S. Patent No. 6,016,476, issued January 18, 2000 (Ex. 1003).
[6] U.S. Patent No. 5,870,723, issued February 9, 1999 (Ex. 1004).
[7] U.S. Patent Publication No. US 2004/0107170 A1, published June 3, 2004 (Ex. 1005).
[8] International Publication WO 01/24123 A1, published April 5, 2001 (Ex. 1006).
[9] U.S. Patent No. 7,865,448 B2, filed October 19, 2004 (Ex. 1007).

II. DISCUSSION

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner and Patent Owner propose very similar statements of the level of ordinary skill in the art. In Patent Owner's phrasing, a skilled artisan would have had "a Bachelor of Science degree in electrical engineering, computer science or computer engineering, and three years of work or research experience in the fields of secure transactions and encryption; or a Master's degree in electrical engineering, computer science or computer engineering, and two years of work or research experience in related fields." PO Resp. 16–17 (citing Ex. 2004 ¶ 18). Petitioner's statement includes only a bachelor's degree and marginally less work experience. Pet. 5. Patent Owner states that its positions would be the same under either party's proposal. PO Resp. 17. We agree with Patent Owner that the analysis and conclusions remain the same under either proposal. As a more-comprehensive definition, we adopt Patent Owner's statement and note that it is consistent with the prior art of record.

B. CLAIM CONSTRUCTION

Petitioner proposes constructions for three terms: "biometric input," "secret information," and "secure registry." Pet. 6–7. Patent Owner asserts that no construction is required for any term. PO Resp. 17.

We agree with Patent Owner that the parties' disputes do not turn on the construction of these terms and construing the claims would not benefit this proceeding. We therefore decline to expressly construe the claims. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (affirming that the Board only need construe claims

terms "to the extent necessary to resolve the controversy") (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

C. UNPATENTABILITY

Petitioner's assertions against the independent claims establish multiple grounds relying on Maes as the primary reference and either Pare or Labrou as the secondary reference. *See* Inst. 9 n.9; Pet. 4. Extending the assertions to dependent claims, Petitioner additionally asserts teachings from Labrou, Pare, and Burger. *See* Inst. 16 n.10, 21; Pet. 4–5. Petitioner also asserts Pizarro as a primary reference, in combination with Pare. Pet. 5.

1. Maes and Pare

Petitioner asserts Maes is prior art under 35 U.S.C. § 102(b) based on its January 18, 2000, issue date. Pet. 7. Maes discloses a system for processing transactions using a "transaction processing device ('personal digital assistant' or 'PDA') in which a user can store his or her credit card, ATM card and/or debit card (i.e., financial) information, as well as personal information, and then access and write selected information to a smartcard ('Universal Card'), which is then used to initiate a POS, ATM, or consumer transaction." Ex. 1003, 2:23–31. User verification on the device "may be performed by using either biometric data, PIN or password, or a combination thereof." *Id.* at 3:59–61.

Maes's device may communicate with a "central server" to obtain a "temporary digital certificate" in order to access a user's information. *Id.* at 2:36–42, 3:38–52. The central server stores personal information, secret information, and biometric data for a user, and verifies a user's identity to issue a digital certificate. *Id.* at 7:20–35. A PDA's connection to the central

server may occur directly through a variety of channels, or may connect via "a special ATM (or other such kiosks)." *Id.* at 7:60–8:5. Maes discloses a user providing verification data to a server to obtain a temporary digital certificate. Ex. 1003, 7:57–10:15. Maes then discloses a number of possible operations to conduct transactions using that digital certificate. Generally, the user's identity is verified on the device, and, if the device has an unexpired digital certificate, the user's payment information is decrypted for use in a transaction. *Id.* at 10:29–11:40. Maes discloses that payment information may be transmitted through a Universal Card (smartcard), or directly through a wireless interface. *Id.* at 12:5–29.

In instances without electronic data transfer, Maes discloses generating an authorization number upon local verification. *Id.* at 12:40–49. The authorization number may be conveyed with card information to a merchant, who uses the authorization number to confirm with the central server that the user is properly verified. *Id.* at 12:30–13:5.

Maes additionally states that "the present invention can be configured to afford an additional level of security for user verification" by verifying the consumer's identity even beyond an unexpired digital certificate and local verification. *Id.* at 13:19–38. In that embodiment for additional security, a file with identifying information is sent from the consumer's device to a POS terminal, which forwards the file to a financial institution. *Id.*

Petitioner asserts Pare is prior art under 35 U.S.C. § 102(b) based on its February 9, 1999, issue date. Pet. 8. Pare discloses a "method and system for tokenless authorization of commercial transactions between a buyer and

a seller using a computer system." Ex. 1004, Abstract. Pare's system verifies buyers by requiring entry of biometric samples and a PIN, sending the information to a remote computer system (the "Data Processing Center (DPC)") in an encrypted state, then comparing the information with such information previously registered by the buyer. *Id.* at 4:14–49, 6:12–16, 8:35–36.

Pare describes using a "Biometric Input Apparatus (BIA)" to "gather, encode, and encrypt biometric input for use in commercial transaction." *Id.* at 10:41–46. For encryption, Pare teaches using a derived unique key per transaction (DUKPT) to select an encryption key from a "Future Key Table" that is an "unpredictable" key. *Id.* at 17:27–55, 18:50–63. The key is used to encrypt the "Biometric-PIN Block," which contains biometric information and a PIN, for transmission to the DPC. *Id.* at 17:29–31.

a. Claim 1

Petitioner maps claim 1's limitations to the references, applying Maes as the primary reference that teaches most claim limitations. *See* Pet. 9–27. While Petitioner asserts further that other references also teach certain limitations, other than as addressed below, we construe the ground as relying on Maes alone.

(1) [Preamble] An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction

Petitioner asserts Maes teaches an electronic ID device allowing a user to store and select various financial cards that comprise a plurality of accounts associated with the user for use in a transaction. Pet. 9–10 (citing Ex. 1003, Abstract, 4:1–5, 12:5–29, Figs. 3, 5, 6). Patent Owner does not

contest Petitioner's assertions in this regard.[10] We need not determine whether the preamble is limiting because we conclude Petitioner has shown Maes teaches the preamble for the reasons provided by Petitioner.

(2) [a] a biometric sensor configured to receive a biometric input provided by the user

Petitioner asserts Maes teaches the claimed biometric sensor. Pet. 11 (citing Ex. 1003, 5:54–63, 3:53–61, 10:49–54, 10:66–11:5, Fig. 1). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed biometric sensor for the reasons provided by Petitioner.

(3) [b] a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts

Petitioner asserts Maes teaches the claimed user interface by disclosing that the central server verifies the user "either biometrically or through PIN or password or a combination thereof" before generating a temporary digital certificate to download onto the user's device. Pet. 12–13 (citing Ex. 1003, 2:59–3:6, 3:45–61, 5:63–67, 8:40–42, 10:18–21, 10:29–44, 10:49–54, 11:5–8, 14:40–46). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed user interface for the reasons provided by Petitioner.

[10] The Scheduling Order instructed: "The patent owner is cautioned that any arguments for patentability not raised in the response will be deemed waived." Paper 16, 7.

(4) [c] a communication interface configured to communicate with a secure registry

Petitioner asserts Maes teaches its PDA includes a communication interface configured to communicate with central server 60, which is a secure registry because it "stor[es] information associated with users, including personal and financial information, a PIN or password, biometric data, and a unique account number, and it performs user verification for transactions." Pet. 13–15 (quoting Ex. 1003, 7:20–41; citing Ex. 1003, 6:60–7:7, 2:59–3:1, 3:42–52, 6:61–7:4, 7:57–8:12, 12:10–57, 13:24–38, Figs. 1, 3). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed communication interface for the reasons provided by Petitioner.

(5) [d] a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface

Petitioner asserts Maes teaches that the user device includes a CPU (a processor) to handle inputs from and issue commands to the various components. Pet. 15–16 (citing Ex. 1003, 5:1–14, Fig. 1). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed processor for the reasons provided by Petitioner.

(6) [d][i] the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information

Petitioner asserts Maes teaches that the user device prohibits access to stored accounts until the user performs local verification using biometric input or a PIN/password. Pet. 17–18 (citing Ex. 1003, 3:45–52, 5:63–67,

10:49–61, 11:9–18, 12:5–29). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed processor programmed to activate the device for the reasons provided by Petitioner.

(7) [d][ii] the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information

Petitioner asserts a combination of teachings from Maes and Pare regarding the processor being "programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information." First, Petitioner looks to Maes's disclosure of generating an authorization number derived from a digital certificate obtained from a central server and using the authorization number to authenticate the user with the server. Pet. 18 (citing Ex. 1003, 12:40–13:5). Petitioner admits that Maes does not teach generating a nonpredictable value or using such a value to generate authentication information. *Id.* For those aspects, Petitioner relies on Pare, which teaches "the concept of generating non-predictable values for generating encrypted authentication information associated with biometric input and secret information." *Id.* In particular, Petitioner looks to Pare's disclosure of a "commercial transaction message" that includes biometric and secret

information, encrypted using a randomly generated key. *Id.* at 19–20 (citing Ex. 1004, 17:27–46, Abstract, 4:34–42, 18:51–61, 19:43–20:15, Fig. 7).

Petitioner asserts that a person of ordinary skill had reason "to substitute the encrypted authentication information taught in Pare . . . for the authorization number of Maes" because Maes already teaches encrypting certain information and discloses that its invention "may employ any known encryption technique or algorithm," and because "encrypting sensitive information had long been an established practice in financial security systems to address fraud." *Id.* at 21–23 (citing Ex. 1003, 10:10–15, 12:66–13:5, 13:24–38, 13:51–60, Fig. 5; Ex. 1009 ¶¶ 54, 36–38).

Patent Owner argues that Petitioner's assertions are deficient for several reasons.

(a) Whether Pare teaches away from the combination

According to Patent Owner, Pare criticizes token-based systems, in which "portable man made memory devices" or "smart cards" store PIN or biometric information, therefore subjecting that information to potential tampering or loss. PO Resp. 20–21 (citing Ex. 1004, 1:12–3:60, 2:21–53, 5:5–8, 6:55–7:3, 7:46–60). Moreover, Patent Owner urges, Pare teaches away from adding security to protect from such risks because doing so "leads to centralization of function" that "looks good during design, but actual use results in increased vulnerability for consumers," "heavier and heavier penalties on the consumer for destruction or loss" of the token, and additional costs. *Id.* at 21 (quoting Ex. 1004, 3:23–36). Patent Owner argues that Pare's "'objective' and 'essence of [the] invention' is to conduct transactions 'without . . . tokens.'" *Id.* (quoting Ex. 1004, 9:12–28; citing Ex. 1004, Abstract, 6:55–7:3, 7:57–60).

Petitioner considers Pare's disclosures, at most, to express a preference for not storing information locally. Reply 4. According to Petitioner, "the encryption techniques of Pare would enhance the security of Maes." *Id.* Petitioner submits that Maes addresses Pare's concern with tokens because of the multiple layers of encryption and authentication imposed to protect the data. Tr. 10:13–18.

"[I]n general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the applicant." *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994). What the prior art teaches, whether a person of ordinary skill in the art would have been motivated to combine references, and whether a reference teaches away from the claimed invention are questions of fact. *Apple Inc. v. Samsung Elecs. Co.*, 839 F.3d 1034, 1051 (Fed. Cir. 2016) (en banc).

We find that Pare does not teach away from using its disclosures in a system such as Maes's because Pare does not discredit token-based systems. Pare's discussion of token-based systems recognizes benefits that arise from such approaches and also presents reasons that Pare's approach is superior. *See* Ex. 1004, 3:2–36. In particular, Pare states that, by adding security, "the resulting system will definitely be more secure." *Id.* Further, Pare's discussion of token-based systems largely focuses on the idea that "the comparison and verification process is not isolated from the hardware and software directly used by the buyer attempting access." *Id.* at 2:22–27. That aspect is not applicable to Maes, which uses remote verification through the digital certificate, as described by Petitioner's application of Maes to the

other limitations of claim 1. Thus, we agree with Petitioner that Maes's system provides features that address Pare's concerns. Tr. 10:13–18; *see* Reply 4 (citing Ex. 1032 ¶¶ 13–14).

Moreover, Petitioner asserts a combination that relies on Pare's teachings "of generating non-predictable values for generating encrypted authentication information associated with biometric input and secret information." Pet. 18. This aspect of Pare is independent of the overall approach used by Maes. We do not read Pare's criticism of token-based systems as indicating that such systems cannot benefit from Pare's encryption techniques. *See KSR Int'l Co. v Teleflex Inc.*, 550 U.S. 398, 420 (2007) ("[F]amiliar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle."). Thus, while Patent Owner argues that Pare teaches a system integrated with a sales terminal rather than a customer device (PO Resp. 22), we do not read Pare's teachings as limited to the particular context in which its system operates.

(b) Whether combining Pare with Maes would be redundant and less secure

Patent Owner argues next that using Pare's methods with Maes would be redundant and less secure. PO Resp. 23. Maes teaches local verification using biometric and PIN entry before proceeding with a transaction. Ex. 1003, 1:10–17, 2:32–42, 3:53–67, 5:60–63, 12:40–47. In contrast, Pare teaches validating biometric and PIN information remotely, at the server. Ex. 1004, Figs. 5, 12; *see also id.* at 2:21–53, 7:46–60. Patent Owner argues that submitting the same information for remote verification "would

needlessly expose the PIN and biometric information to fraud." PO Resp. 25–26 (citing Ex. 2004 ¶ 61).

Petitioner argues in response that skilled artisans would have configured a system to perform multiple verifications because it would enhance security. Reply 5 (citing Ex. 1032 ¶¶ 15–20). Petitioner points out that Maes discloses remote verification when downloading a digital certificate, along with local verification before decrypting the certificate, and that Maes may be configured to require verification of the certificate for each transaction. Reply 5–6 (citing Ex. 1003, 8:50–65, 10:18–21, 3:59–61, 5:54–67; Ex. 1032 ¶ 18). Petitioner points out additionally that Maes teaches the remote server confirming a transaction using an "authorization number, which is a function of the digital certificate." *Id.* at 6 (citing Ex. 1003, 12:66–13:4, 6:50–53; Ex. 1032 ¶ 19).

We find that, although Petitioner's asserted combination would implement redundant authentication, skilled artisans had reason to make the combination. Indeed, it is because of the redundant authentication that the proposed combination would have enhanced security. Reply 9. Further, Maes's teachings regarding local and remote verification of digital certificates are consistent with the combination incorporating Pare's methods for remote verification. *See* Ex. 1003, 3:36–42, 3:39–49, 3:59–61. Although Patent Owner's declarant takes the position that Maes's remote and local verification occur at different time points, Maes discloses a user may choose the lifetime for a certificate, including requiring a new certificate for each transaction. Ex. 1033, 81:23–82:21; Ex. 1032 ¶ 18. Using

Pare's teachings to modify Maes's remote verification process would have improved security as asserted by Petitioner.

(c) Whether combining Pare with Maes would eliminate important features of Maes and change Maes's principles of operation

Patent Owner argues that replacing Maes's authorization number with Pare's transaction message would eliminate Maes's ability to "provide[] biometric security for transactions that do not involve electronic data transfer" because the combined system would no longer display an authorization number on the screen. PO Resp. 27 (modification in original) (quoting Ex. 1003, 12:30–54). According to Patent Owner, that ability is a key feature of Maes that enables it to work with existing infrastructure. *Id.* at 28–29.

Petitioner responds that the ability to be used in transactions without electronic data transfer is not a basic principle of Maes, as shown by Maes's embodiment with electronic transmission for the authorization number. Reply 7–8 (citing Ex. 1003, 14:58–67). Instead, Petitioner asserts, Maes's basic principle is centrally verified transactions that eliminate the need to carry insecure cards. *Id.* at 7 (citing Ex. 1032 ¶ 21; Ex. 1003, 1:59–2:20, 2:23–30, 3:32–37). According to Petitioner, because Maes's authorization number is derived from a server-issued certificate, it "allow[s] the central server to confirm for the merchant that the user was properly verified with the server." Reply 8 (quoting Ex. 1032 ¶ 23).

We find that the asserted combination would not change Maes's principle of operation. Significantly, Patent Owner relies on one aspect of an embodiment to assert that the combination would impermissibly change Maes by removing the ability to convey an authorization number orally.

PO Resp. 27–28. But at least certain of Maes's embodiments do involve electronic data transfer. Ex. 1003, 12:9–13 ("[T]he consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ATM or POS transaction terminal through an established communication link."); *see also id.* at 3:34–36 ("The PDA is also capable of transmitting or receiving information through wireless communications such as radio frequency (RF) and infrared (IR) communication."), 13:34–38 ("The selected card information, as well as the encrypted information file, would be transmitted to the POS terminal (via the Universal Card, RF or IR) . . . ."). We agree with Petitioner that Maes's principle of operation is to provide transaction security through: (1) client-server interaction to authenticate a device with a server; and (2) local interaction to verify a user with the device. *See* Ex. 1003, 1:23–42.

Although Petitioner's proposed modification would eliminate Maes's applicability to transactions without electronic data transfer, losing that feature does not preclude a conclusion of obviousness. *See Allied Erecting & Dismantling Co. v. Genesis Attachments, LLC*, 825 F.3d 1373, 1381 (Fed. Cir. 2016) ("Although modification of the movable blades may impede the quick change functionality disclosed by Caterpillar, '[a] given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine.'") (quoting *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006)). Because Petitioner's proposed modification of Maes does not impact Maes's fundamental purpose of security through both central and local verification, we find the combination would not change Maes's principle of operation.

Patent Owner argues further that the combination would require infrastructure changes, also contrary to Maes's teachings. PO Resp. 28–30. Patent Owner relies on Maes's statement that one of its objects is to provide a PDA device that is "compatible with the current infrastructure (i.e., immediately employed without having to change the existing infrastructure)." *Id.* at 28 (quoting Ex. 1003, 2:43–49). According to Patent Owner, the infrastructure existing at the time of invention was not compatible with Pare's protocol because its commercial transaction message would require changes to multiple elements in Maes's system. *Id.* at 29 (citing Ex. 2004 ¶ 65). Further, because one aspect of Pare's system requires merchant identification using a seller code, Patent Owner asserts the system is inconsistent with Maes's goal of a PDA device that works with existing infrastructure. *Id.* at 29–30.

Petitioner responds that Maes teaches that its PDA may be used without the "Universal Card" that enables use of existing infrastructure by interacting with "electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities without even having to use the Universal Card." Ex. 1003, 12:5–8; Reply 8 (citing Ex. 1003, 12:5–29). Petitioner points out that Maes contemplates a range of specialized systems, including "'advanced' POS terminals that write receipts to cards or PDA or 'special' POS terminals with biometric sensors." Reply 8 (citing Ex. 1003, 11:42–51, 12:16–18, 14:17–21). Petitioner's argument is persuasive because Maes contemplates applications in which some changes are required to the existing infrastructure. Therefore, Patent Owner's assertion is not correct—such changes are not contrary to Maes's

fundamental operation. As a matter of degree—that any required changes do not rise to a level that show skilled artisans would not have made the combination—we agree with Petitioner.

Regarding Pare's use of a seller code, Petitioner submits that adapting Maes's system to incorporate such a feature would have been a minor software modification with predictable results. Reply 9 (citing Ex. 1032 ¶ 25). We agree that the nature of accommodating such a change, in light of Maes's contemplation of infrastructure changes in some embodiments, would not have discouraged skilled artisans from making the asserted combination.

(d) Whether Petitioner provides an adequate reason how or why to combine Pare with Maes

Beyond the above arguments that combining Pare with Maes would be improper, Patent Owner argues that Petitioner fails to provide an adequate reason to combine the references. PO Resp. 30–34. As an initial matter, we do not agree with Patent Owner that Petitioner must have identified a "deficiency or weakness in Maes that would motivate a POSITA to modify the reference." *See id.* at 31. Such a rule would contradict the Supreme Court's instruction that "when a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result." *KSR*, 550 U.S. at 416.

As summarized above, Petitioner asserts that using Pare's encrypted authentication information in place of Maes's authorization number was a substitution of one known technique for another with a predictable result. Pet. 18, 21–23 (citing Ex. 1003, 10:10–15, 12:66–13:5, 13:24–38, 13:51–60,

Fig. 5; Ex. 1009 ¶¶ 54, 36–38). Petitioner offers a persuasive view of Maes and Pare in which both use information to authenticate a user with a remote system. In Maes, the authorization number is used to authenticate a user. Ex. 1003, 12:55–13:5. Similarly, Pare's transaction message is used to authenticate a user. Ex. 1004, 4:37–42. Thus, we agree with Petitioner that skilled artisans had reason to use Pare's method in place of Maes's as an alternative, known method of authenticating users. Pet. 18, 21–23. We further agree with Petitioner that the combination would have had a predictable result in light of the similarities between Maes and Pare and the relatively minor changes required to make the combination. *Id.* at 22–23.

Beyond asserting the combination is a straightforward substitution of one authentication method for another, Petitioner further points out that Maes teaches encrypting a user's information for transmission. *Id.* at 21–22 (citing Ex. 1003, 13:24–38). Petitioner relies also on Maes's statement that "the present invention may employ any known encryption technique or algorithm for the encryption/decryption process." Pet. 22 (quoting Ex. 1003, 10:10–15). Patent Owner argues that although Maes teaches encrypting certain information for transfer, it does not teach encrypting the authorization number. PO Resp. 32 (citing Ex. 1003, 12:30–39, 6:42–55). Petitioner, on the other hand, submits that because Maes's authorization number "already represents obscured data" (as a function of the digital certificate issued by the server), there is no need to further encrypt the authorization number. Reply 10 (citing Ex. 1032 ¶ 28). We agree—Petitioner's reliance on Maes's encryption discussion makes sense because although no encryption is required for an authorization number (which

contains no identifying information), it is required when transmitting other types of information, and Maes discloses using encryption in such instances. *See* Reply 10. Based on the evidence above, we find that skilled artisans would have had reason with rational underpinning to use Pare's authentication technique, including the more-specific encryption it teaches, in Maes's system.

(8) [d][iii] [processor is configured . . .] to communicate the encrypted authentication information via the communication interface to the secure registry

Regarding the requirement to "communicate the encrypted authentication information via the communication interface to the secure registry," Petitioner asserts that, although Maes discloses that its "authorization number may be displayed or verbally communicated to a merchant," a person of ordinary skill would have found it obvious "that this number could be transmitted wirelessly." Pet. 23–24. Petitioner further asserts that Pare teaches the wireless-transmission limitation. *Id.* at 24 (citing Ex. 1004, 4:34–58, 6:12–17, 23:60–24:17, 30:63–31:27, Figs. 17–18).[11] Petitioner contends that a person of ordinary skill would have applied these

[11] As discussed in the Institution Decision, we understand this aspect of Petitioner's challenge as continuing to rely on Pare and Labrou in each of the respective challenges. Inst. 13–14. In the ground applying Maes and Pare, we interpret Petitioner's challenge as relying on Pare's teaching of communicating the authentication information to the secure registry, as combined with Maes; likewise, in the ground applying Maes and Labrou, we interpret Petitioner's challenge as relying on Labrou's teaching of that limitation, as combined with Maes. This understanding applies also to the limitations requiring wireless transmission to a point-of-sale device and that the secure registry be configured to receive authentication information from the point-of-sale device.

teachings to Maes's system because Pare's system "perform[s] the functions of storing information related to users and authenticating transactions, just as the secure registry in the '813 Patent and the central server in Maes" and because "Maes itself already contemplates that authentication information may be wirelessly communicated to the central server for verification using the POS device as a conduit." *Id.* at 24–25 (citing Ex. 1009 ¶¶ 40, 50, 52, 54–56).

Patent Owner's challenge to Petitioner's assertions is subsumed within its arguments discussed above, in that Patent Owner argues there was no reason to look to Pare's system and apply its teachings to Maes. PO Resp. 18–34. As discussed, we do not find those arguments persuasive. Further, we find Petitioner shows that a skilled artisan using Pare's method in place of Maes's authorization number would also have configured the system to communicate the authentication information via the communication interface to the secure registry, because both Maes and Pare disclose transmitting information electronically, other than Maes's particular embodiment where an authorization number is used for nonelectronic transactions. Pet. 24–25 (citing Ex. 1003, Abstract, 13:34–38; Ex. 1004, Abstract, 4:34–58, 6:12–17, 23:60–24:17, 30:63–31:27; Ex. 1009 ¶¶ 50, 54–56).

(9) [e][i] wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and

Petitioner relies on Maes's disclosure that its PDA may transmit information to a POS device wirelessly. Pet. 25–26 (citing Ex. 1003, 12:5–16, 12:17–29, Abstract, 3:34–36, 8:5–10, Fig. 1). Patent Owner does not

contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed communication interface for the reasons provided by Petitioner.

(10) [e][ii] wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device

Regarding the requirement to transmit the authentication information to the secure registry via a POS device, Petitioner relies on Maes's disclosures that its "invention may interact with electronic fund transfer systems or transaction terminals having wireless or direct communication capabilities" and that "the consumer transaction may be performed by transmitting the selected card information directly from the PDA device to the ATM or POS transaction terminal through an established communication link L2." Pet. 25–26 (quoting Ex. 1003, 12:5–16). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Maes teaches the claimed secure registry for the reasons provided by Petitioner.

(11) Conclusion

Petitioner has shown by a preponderance of the evidence that the combination of Maes and Pare teaches the limitations of claim 1 and that skilled artisans would have had reason with rational underpinning to combine Maes's and Pare's teachings as asserted. Patent Owner's arguments against those findings are not persuasive. Further, Patent Owner has not offered objective evidence of nonobviousness to weigh against Petitioner's

evidence of obviousness.[12] We conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 1 would have been obvious to a person of ordinary skill in the art over Maes and Pare.

b. Claims 16 and 24

Independent claims 16 and 24 are directed to methods of "generating authentication information" and of "controlling access to a plurality of accounts," respectively, and recite limitations parallel to those of claim 1. Petitioner maps the limitations of claims 16 and 24 to the prior art in the same manner Petitioner mapped the limitations of claim 1. Pet. 33–35, 38–40. Patent Owner does not raise additional arguments specific to claims 16 or 24. For the reasons discussed above regarding claim 1, and for the reasons presented in the Petition, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 16 and 24 would have been obvious to a person of ordinary skill in the art over Maes and Pare.

c. Claim 2

Claim 2 depends from claim 1 and recites further that "the electronic ID device comprises a discrete code associated with the electronic ID device." Petitioner asserts that Maes teaches the additional limitation of claim 2 by disclosing "that each user's PDA can include a universal card that is assigned a 'unique Universal Card number.'" Pet. 27 (citing Ex. 1003, 3:27–32, 6:36–41, 7:45–49). When performing wireless transactions, Maes

[12] This aspect of Patent Owner's case applies equally to all grounds in this proceeding.

discloses that "the PDA device 10 itself actually takes the place of the Universal Card 26." *Id.* at 27–28 (quoting Ex. 1003, 12:23–29).

Patent Owner argues that Maes's Universal Card number is not a "discrete code associated with the electronic ID device" because the universal card number is associated with the Universal Card, not the PDA, and because the account number is not unique to a particular PDA. PO Resp. 35–38. Petitioner responds that (1) claim 2 requires only that the discrete code be "associated with" the device, not that it be unique to the device, and (2) Maes discloses that the account number is "of the PDA device." Reply 11 (quoting Ex. 1003, 7:45–49).

We agree with Petitioner. Patent Owner does not justify its position that a discrete code must be unique to the device with which it is associated. Although the '813 patent Specification discusses a unique number (*see* Ex. 1001, 47:1–5), claim 2 recites only that the discrete code is "associated with the electronic ID device" and Patent Owner has not provided adequate reason to import a requirement for uniqueness. Further, Maes states that the account number is unique to the Universal Card. Ex. 1003, 7:25–27. Although Patent Owner argues that Maes's account number would change with issuance of a new Universal Card (PO Resp. 38), that does not mean that the new number is not unique. Rather, replacing the card would change the account number of the Universal Card and the PDA device together.

We conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 2 would have been obvious to a person of ordinary skill in the art over Maes and Pare.

d. Claims 3, 5, and 11

Claim 3 depends from claim 1 and recites that "at least a portion of the biometric input received by the biometric sensor is communicated to the secure registry for authentication prior to generation of the encrypted authentication information." Claim 5 depends from claim 1 and recites "a memory coupled to the processor, wherein the memory stores information employed by the electronic ID device to authenticate the biometric received by the biometric sensor." Claim 11 depends from claim 1 and recites that "the biometric sensor is configured to receive and process at least one of a fingerprint, a speech/voice input, an iris scan, a retina scan, a facial scan, written information and a DNA input." Petitioner maps the limitations of dependent claims 3, 5, and 11 onto Maes's disclosures. Pet. 28–31. Patent Owner makes no arguments relevant to these claims beyond those discussed above for claims 1 and 2. *See generally* PO Resp. 18–38.

Maes discloses that "biometric data[,] such as voice prints (models) of the user, are also stored in the central server 60 of the service provider for user verification during the client/server mode to obtain a digital certificate." Ex. 1003, 7:27–31. We agree with Petitioner that that disclosure teaches the additional limitations of claim 3. Maes discloses memory connected to its CPU (*id.* at Fig. 1), used to store information for authenticating biometric information (*id.* at 10:57–61), and we agree that disclosure teaches the additional limitations of claim 5. Maes discloses a biometric sensor "to collect biometric data to be processed by the biometric processor module 22 using known techniques, e.g., finger, thumb or palm print data, handwriting data, a retinal vascular pattern data or a combination thereof" (*id.* at 10:66–

11:5) and we agree that that disclosure teaches the additional limitations of claim 11.

We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 3, 5, and 11 would have been obvious to a person of ordinary skill in the art over Maes and Pare, for the reasons given by Petitioner. *See* Pet. 28–31.

e. Claim 20

Claim 20 depends from claim 16 and recites "generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by a secure registry." Petitioner asserts that Pare "teaches that a transaction message will include an 'account index code' with which the computer system can identify the selected account to charge for the transaction." Pet. 36 (citing Ex. 1004, 4:38–39, Fig. 18). Petitioner asserts that a person of ordinary skill had reason "to incorporate Pare['s] . . . teachings of generating encrypted authentication information to allow user and account identification by a secure registry into the system of Maes in order to secure a user's confidential account information" and "to prevent potential hackers or unethical merchants from discovering this confidential information." *Id.* at 37 (citing Ex. 1009 ¶ 57).

Patent Owner makes no arguments for patentability of claim 20 beyond those discussed above for claim 1. *See generally* PO Resp. We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 20 would

have been obvious to a person of ordinary skill in the art over Maes and Pare, for the reasons given by Petitioner. *See* Pet. 36–37.

f. Claims 13–15, 17, 22, 23, 25, and 26

Claim 13 depends from claim 1 and recites that "the processor is configured to display indicators for the plurality of accounts in the user interface, and the user interface is configured to accept user selection of a respective one of the plurality of accounts"; claim 17 recites a parallel limitation. Petitioner asserts that Maes teaches the limitations of claims 13 and 17 by disclosing that a "desired card may be selected through the user interface/display 34." *Id.* at 32. Petitioner, however, provides no explanation or support for such a conclusion. *Id.* Patent Owner makes no arguments for patentability of claim 13 or 17 beyond those discussed above for claim 1. *See generally* PO Resp. 18–38. We conclude that Petitioner has not shown adequately that the disclosure in Maes teaches all aspects of the limitations of claims 13 and 17. *See Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1364 (Fed. Cir. 2016) (holding that a petitioner does not satisfy its burden by simply stating, without explanation, that a disclosure in the art satisfies a claim limitation).

Claim 14 depends from claim 1 and recites that "the user interface is configured to display options for purchase"; claims 22 and 25 depend from claims 16 and 24, respectively, and recite parallel limitations. Claim 15 depends from claim 14 and recites that "the user interface is configured to accept selection of at least one product or service"; claims 23 and 26 depend from claims 22 and 25, respectively, and recite parallel limitations. Petitioner asserts that Maes teaches the limitations of claims 14, 22, and 25, and those of claims 15, 23, and 26 because it discloses "the user device may

be used for transactions on a merchant's web site." Pet. 40 (citing Ex. 1003, 13:39–50, 14:1–16). Patent Owner makes no arguments for patentability of claim 14, 15,22, 23, 25, or 26 beyond those discussed above for claim 1. *See generally* PO Resp. 18–38. We are not persuaded that using a device for transactions on a website would necessarily satisfy the limitations of claims 14, 22, and 25, or those of claims 15, 23, and 26. Petitioner provides no explanation of why that would be so, either in the Petition or through declaration testimony. *See* Pet. 40. We therefore conclude that Petitioner has not shown adequately that the disclosure in Maes teaches the limitations of any of claims 14, 15, 22, 23, 25, and 26.

2. Maes and Labrou

Petitioner asserts Labrou is prior art under 35 U.S.C. § 102(b) based on its June 3, 2004, publication date. Pet. 8. Labrou discloses a "computer system for conducting purchase transactions using wireless communications between a consumer and a merchant." Ex. 1005, Abstract. Labrou's system employs a "Secure Transaction Server (STS 106) . . . for deciding which transaction requests are legitimate and passes them to the payment service of a financial institution." *Id.* ¶ 119. Labrou discloses encrypting a user's transaction information in part using a "Private Identification Entry (PIE)," which is a "shared secret input by the user" and may be a PIN or "may be deterministically generated using a biometric device such as a fingerprint sensor." *Id.* ¶ 524. The PIE is used in combination with a "Random Sequence Number (RSN)" to create an encryption key. *Id.* ¶¶ 253, 527, 535–537. The STS decrypts messages from the user's device and the merchant's device and validates transaction information. *Id.* ¶¶ 258–261.

a. Claim 1

Petitioner maps claim 1's limitations to the references, applying Maes as the primary reference that teaches most claim limitations. *See* Pet. 9–27. While Petitioner asserts further that other references also teach certain limitations, we construe the ground as relying on Maes alone, other than as addressed below. Therefore, we reach the same conclusions regarding Maes for the same reasons as for the ground based on Maes and Pare, above. We address Petitioner's reliance on Labrou below.

(1) [d][ii] the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information

Petitioner asserts that Labrou renders obvious "the concept of generating non-predictable values for generating encrypted authentication information associated with biometric input and secret information." Pet. 18. Petitioner relies on Labrou's disclosure of encrypting transaction information using: (1) a "Private Identification Entry (PIE)," which may be input as a PIN or determined from biometric information; and (2) a "random sequence number (RSN)," which Petitioner asserts is a nonpredictable value. *Id.* at 20–21 (citing Ex. 1005 ¶¶ 253, 259, 524, 527, 535–537). Petitioner asserts that skilled artisans had reason to use both a PIN and biometric information to generate Labrou's PIE, and had reason to use the encrypted transaction information in place of Maes's authorization number. *Id.* at 18, 20–22.

(a) Using both a PIN and biometric information in Labrou's PIE

Petitioner asserts it would have been obvious to a person of ordinary skill in the art to use *both* a user-entered PIN and biometric information to generate Labrou's PIE, because Labrou "already teaches that both sets of information may be used together to authenticate a user" and because "doing so would have further enhanced the security of transactions in Labrou by creating an additional layer of security." *Id.* at 21 (citing Ex. 1005 ¶¶ 421, 158; Ex. 1009 ¶¶ 53–54). Patent Owner challenges that assertion, arguing there was no motivation to modify Labrou to use both a PIN and biometric information. PO Resp. 40–44. We agree with Petitioner that, in light of Labrou's disclosure that biometric and PIN information may be used together (*see* Ex. 1005 ¶ 421), and a desire to maximize security, skilled artisans had reason with rational underpinning to configure a system to use both types of information when generating Labrou's PIE.

Patent Owner argues also that Labrou fails to teach "how to implement the PIE using a biometric" and therefore cannot teach the limitation. PO Resp. 41–43. That argument, however, is one that Labrou does not enable the use of biometric information in a PIE, and cannot overcome an assertion of obviousness. *See ABT Sys., LLC v. Emerson Elec. Co.*, 797 F.3d 1350, 1360 n.2 (Fed. Cir. 2015) ("ABT's suggestion that Cornelius and Nakatsuno are non-enabled is misplaced, since even '[a] non-enabling reference may qualify as prior art for the purpose of determining obviousness,' and even 'an inoperative device . . . is prior art for all that it teaches.'" (quoting *Symbol Techs., Inc. v. Opticon, Inc.*, 935 F.2d 1569, 1578 (Fed. Cir. 1991); *Beckman Instruments, Inc. v. LKB Produkter AB*, 892 F.2d 1547, 1551 (Fed. Cir. 1989))). Labrou discloses that biometric

information may be used to deterministically generate a PIE (Ex. 1005 ¶ 524) and we determine that disclosure satisfies the claim language ("information associated with at least a portion of the biometric input").

Patent Owner argues further that Labrou teaches using biometric and PIN input only for locally authenticating a user to the device. PO Resp. 43–44 (citing Ex. 1005 ¶¶ 283–284). We agree that Labrou discusses biometric input as a possible method of locally authenticating a user. But Petitioner relies also on Labrou's disclosure that a user completing a transaction (i.e., a user already locally authenticated to a device) enters a "PIN (and/or biometric if available)." Pet. 21 (quoting Ex. 1005 ¶ 421). That disclosure indicates that the transaction may use both PIN and biometric information, and it supports that using both PIN and biometric information together may be beneficial. Further, we agree with Petitioner that skilled artisans would have understood that using both PIN and biometric information would create an additional layer of security. Ex. 1009 ¶ 53–54.

Thus, we conclude that Petitioner has shown a person of ordinary skill would have had reason with rational underpinning to use Labrou's teachings such that Maes's device modified in light of those teachings would generate encryption information using both a PIN and biometric information.

(b) Using Labrou's encrypted authentication information with Maes's system

Next, as to using Labrou's PIE with Maes's system, Petitioner asserts that a person of ordinary skill had reason "to substitute the encrypted authentication information taught in . . . Labrou for the authorization number of Maes" because Maes already teaches encrypting certain information and discloses that its invention "may employ any known encryption technique or

algorithm," and because "encrypting sensitive information had long been an established practice in financial security systems to address fraud." Pet. 21–23 (citing Ex. 1003, 10:10–15, 12:66–13:5, 13:24–38, 13:51–60, Fig. 5; Ex. 1009 ¶¶ 54, 36–38). Patent Owner argues that Petitioner has not explained how the combination would function (PO Resp. 45–46) and has not adequately justified making the combination for the same reasons Patent Owner raises against the combination of Maes and Pare (*id.* at 46–48). We conclude that Petitioner adequately justifies combining Labrou's teachings with Maes for the same reasons discussed above, which rely on Maes and therefore apply to Labrou just as they apply to Pare. *See supra* at 21–23.

Regarding how the combination of Maes and Labrou would work, Patent Owner argues that Labrou teaches two types of "encrypted authentication information" (consumer messages and merchant messages) and that the Petition is unclear which or both would be substituted into Maes's system in place of the authorization number. PO Resp. 45–46. Patent Owner's complaint is misplaced because the Petition states that, in Labrou, "a user's transaction information is encrypted by the user's device using a 'Private Identification Entry (PIE).'" Pet. 20 (citing Ex. 1005 ¶¶ 253, 259, 527, 535–537); Reply 15 (citing Pet. 20–21, 24–25, 34). Labrou describes how "the consumer device 102 generates the encrypted part of the consumer message" (Ex. 1005 ¶ 253) and therefore makes clear that Petitioner asserts using Labrou's consumer message in the combination. Thus, we conclude Petitioner has shown adequately how a person of ordinary skill would have configured the asserted combination.

Accordingly, we conclude that Petitioner has shown a person of ordinary skill would have had reason with rational underpinning to use Labrou's teachings regarding the encrypted consumer message in combination with Maes's system.

(2) [d][iii] [processor is configured . . .] to communicate the encrypted authentication information via the communication interface to the secure registry

Beyond the reasoning discussed above regarding Maes (*see supra* at 23), Petitioner asserts further that Labrou teaches the wireless-transmission limitation. *Id.* at 24 (citing Ex. 1005, Abstract, ¶¶ 188–190, 210–212, 322–323). Petitioner contends that a person of ordinary skill would have applied these teachings to Maes's system because Labrou's system "perform[s] the functions of storing information related to users and authenticating transactions, just as the secure registry in the '813 Patent and the central server in Maes" and because "Maes itself already contemplates that authentication information may be wirelessly communicated to the central server for verification using the POS device as a conduit." *Id.* at 24–25 (citing Ex. 1009 ¶¶ 40, 50, 52, 54–56).

Other than as discussed above regarding the combination of Labrou and Maes generally, and regarding the justification based on Maes's teachings (discussed regarding combination with Pare, *see supra* at 21–23), Patent Owner does not specifically challenge Petitioner's assertions regarding how the combination would transmit authentication information. We find Petitioner has shown Labrou teaches the claimed communication for the reasons provided by Petitioner.

(3) Conclusion

Petitioner has shown by a preponderance of the evidence that the combination of Maes and Labrou teaches the limitations of claim 1 and that skilled artisans would have had reason with rational underpinning to combine Maes's and Labrou's teachings as asserted. Patent Owner's arguments against those findings are not persuasive. Further, Patent Owner has not offered objective evidence of nonobviousness to weigh against Petitioner's evidence of obviousness. We conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 1 would have been obvious to a person of ordinary skill in the art over Maes and Labrou.

b. Claims 16 and 24

Independent claims 16 and 24 are directed to methods of "generating authentication information" and of "controlling access to a plurality of accounts," respectively, and recite limitations parallel to those of claim 1. Petitioner maps the limitations of claims 16 and 24 as it does those of claim 1. Pet. 33–35, 38–40. Patent Owner does not raise arguments specific to claims 16 or 24. For the reasons discussed above regarding claim 1, and for the reasons presented in the Petition, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 16 and 24 would have been obvious to a person of ordinary skill in the art over Maes and Labrou.

c. Claims 2, 3, 5, 11

As discussed above, Petitioner persuasively maps the additional limitations of claims 2, 3, 5, and 11 to Maes's disclosures. *See supra* at 26–29. Patent Owner makes no arguments relevant to these claims beyond those

discussed above for claim 1. *See generally* PO Resp. 38–58. Thus, for the reasons discussed above regarding Maes and Pare, we conclude Petitioner has shown by a preponderance of the evidence that the subject matter of claims 2, 3, 5, and 11 would have been obvious over Maes and Labrou. *See supra* at 26–29.

d. Claims 12 and 21

Claim 12 depends from claim 11 and recites that:

> the processor is configured to generate account identifying information for the respective one of the plurality of accounts wherein the account identifying information does not identify an account number of the respective one of the plurality of accounts.

Claim 21 depends from claim 16 and recites a parallel limitation.

Petitioner asserts that Labrou teaches these limitations and that a person of ordinary skill in the art had reason "to incorporate Labrou's teachings of generating account aliases, rather than account numbers, to identify one of a plurality of accounts into the system of Maes at least to further Maes's objective of preventing unauthorized access of a consumer's confidential account information." Pet. 31 (citing Ex. 1005 ¶¶ 293, 532, Figs. 52–55; Ex. 1009 ¶ 59); *accord id.* at 37–38.

Patent Owner argues that Labrou's account aliases do not meet these claim limitations because the aliases are not generated after one of the accounts is selected. PO Resp. 49–50. Because aliases used to select an account in Labrou are generated prior to an account being selected, according to Patent Owner, they cannot be the claimed account identifying information. *Id.* Petitioner responds that Patent Owner applies an incorrect

claim construction to require generation of account identifying information after selection of the account. Reply 15–16.

We agree with Patent Owner that the language of claim 12 requires the claimed device generate account identifying information only *after* selection by a user. Claim 12 recites that the processor generates information "for the respective one of the plurality of accounts," a phase that refers back to "an account selected by the user from the plurality of accounts." Thus, the language of claim 12 logically requires generating account identifying information only after selection of an account by the user from a plurality of accounts. In Labrou, aliases for accounts are displayed on the screen for a user to select, so the aliases were generated prior to selection. Ex. 1005 ¶ 293.

Petitioner asserts also that, once an alias is selected, information about the alias is sent to the server, which then correlates the alias to an account (generating account identifying information). Reply 16 (citing Ex. 1032 ¶ 31). In Petitioner's theory, Labrou's user device would "generate information specifying the particular alias that had been selected" to send to the server. Ex. 1032 ¶ 31. But Petitioner's declarant also states that the alias itself would be account identifying information. *Id.* ¶ 32. Petitioner does not adequately justify reading the claim language on copying an account alias into a message sent to the server. Thus, we conclude Petitioner has not shown that the subject matter of claim 12 or 21 would have been obvious over Maes and Labrou.

e. Claims 13–15, 17, 22, 23, 25, and 26

In addition to its assertions based on Maes, discussed above (*see supra* at 30), Petitioner maps the limitations of claims 13–15, 17, 22, 23, 25,

and 26 onto Labrou's teachings. Regarding claims 13 and 17, Petitioner asserts a person of ordinary skill had reason "to incorporate Labrou's teachings of a user interface displaying indicators for a plurality of accounts and accepting selection of one of the accounts because a PHOSITA would have appreciated that this would enhance the usability of the device." Pet. 32 (citing Ex. 1005 ¶ 293, Figs. 52–55; Ex. 1009 ¶ 60); *accord id.* at 36. Patent Owner does not contest Petitioner's assertions in this regard.

Regarding claims 14, 15, 22, 23, 25, and 26, Petitioner asserts a person of ordinary skill in the art had reason "to incorporate Labrou's teachings of displaying options for selection and purchase on a user interface into the system of Maes because, as mentioned, Maes contemplates that the user device may be used for purchasing items over the Internet." Pet. 40 (citing Ex. 1005 ¶ 157, 161 ("[T]he device 102 displays to the user available services (merchants and services that the merchant offers) and the user navigates through the offered services and selects which one to interact with."); Ex. 1009 ¶ 61). As noted in the Institution Decision (Inst. 18–19), we interpret Petitioner as asserting that using Labrou's teachings for an action already taught by Maes would have been a simple substitution. *See KSR*, 550 U.S. at 416 ("[W]hen a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result."). Patent Owner does not contest Petitioner's assertions in this regard.

For the reasons presented in the Petition, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of

claims 13–15, 17, 22, 23, 25, and 26 would have been obvious to a person of ordinary skill in the art over Maes and Labrou.

f. Claim 19

Claim 19 depends from claim 16 and further recites "an act of generating a seed from which the authentication information is generated by employing at least two of the biometric data, the secret information known to the user, and an electronic serial number of the electronic ID device." Petitioner asserts that Labrou teaches these limitations for the same reasons it teaches the similar limitations of claim 10. Pet. 36, 45–46.

Petitioner maps the limitations of claim 19 onto Labrou's teachings, asserting a person of ordinary skill in the art had reason "to incorporate the teachings of Labrou into the system of Maes as a known way to generate a non-predictable value, such as a random number, from a seed because the use of seeds to generate random numbers for encrypting information was well known in the art, as evidenced by the ANSI X9.17 standard." Pet. 44–46 (regarding claim 10). We stated in the Institution Decision that Petitioner's assertion was inadequate because it established only that such teachings were known, not that there was a reason to use them in combination with teachings of another reference. Inst. 19–20; *see also* PO Resp. 56–58. Petitioner does not pursue unpatentability of claim 19 in the Reply. *See generally* Reply. We reach the same conclusion here, for the same reason we stated in the Institution Decision. Accordingly, we conclude Petitioner has not shown that the additional subject matter of claim 19 would have been obvious over Labrou.

g. Claim 20

Claim 20 depends from claim 16 and recites "generating encrypted authentication information in a manner that allows the identification of the user and the selected one of the plurality of user accounts by a secure registry." Petitioner asserts also that Labrou "teaches that encrypted agreement data will contain information regarding the selected financial account." Pet. 36 (citing Ex. 1005 ¶ 532). Labrou discloses that "agreement data conveys the specific details that are agreed upon by the involved parties" and may include "the financial account with which one party agrees to pay the second party." Ex. 1005 ¶ 532. Petitioner asserts that a person of ordinary skill had reason "to incorporate . . . Labrou's teachings of generating encrypted authentication information to allow user and account identification by a secure registry into the system of Maes in order to secure a user's confidential account information" and "to prevent potential hackers or unethical merchants from discovering this confidential information." Pet. 37 (citing Ex. 1009 ¶ 57).

Patent Owner does not raise any arguments for the patentability of claim 20 beyond those applicable to the independent claims. *See generally* PO Resp. 38–58. We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 20 would have been obvious to a person of ordinary skill in the art over Maes and Labrou, for the reasons given by Petitioner. *See* Pet. 36–37.

3. Maes, Pare, and Labrou

In the Institution Decision, we identified that Petitioner challenged claims 12–15, 17, 19–23, 25, and 26 over Maes, Pare, and Labrou. Inst. 16, 17, 19, 20, 21. Petitioner asserts that Labrou's teachings regarding the limitations of those claims apply to Maes combined with Pare just as they apply to Maes combined with Labrou. *See* Pet. 31, 32, 36–38, 44–46; Inst. 16 n.10.

For this ground, Patent Owner relies on its arguments for the independent claims. PO Resp. 59. Thus, for the reasons discussed above regarding these claims in light of Maes and Labrou, we conclude: (1) Petitioner has not shown that the subject matter of claim 12, 19, or 21 would have been obvious over Maes, Pare, and Labrou (*see supra* at 38, 41); and (2) Petitioner has shown that the subject matter of claims 13–15, 17, 20, 22, 23, 25, and 26 would have been obvious over Maes, Pare, and Labrou (*see supra* at 39).

4. Maes, Pare, and Burger

Petitioner asserts Burger is prior art under 35 U.S.C. § 102(b) based on its April 5, 2001, publication date. Pet. 41. Burger discloses an apparatus called a "Pocket Vault" for authorizing users and providing transaction information to a point-of-sale terminal. Ex. 1006, 2:15–20, 11:12–20. Burger's Pocket Vault requires a user to use his or her fingerprint to access most of the functionality of the device, other than limited functions such as retrying the fingerprint entry or accessing device return information or emergency information. *Id.* at 29:31–30:25; 33:5–35:15, Fig. 7.

Patent Owner relies on its challenges to the independent claims and does not otherwise contest Petitioner's assertions regarding the combination of Maes, Pare, and Burger. PO Resp. 59.

a. Claim 6

Claim 6 depends from claim 5 and recites, "the electronic ID device does not permit the entry of the user input if the biometric input received by the biometric sensor is determined to not belong to an authorized user of the electronic ID device." Petitioner asserts that Burger teaches this limitation by disclosing a device requiring fingerprint-based authorization where, "if the fingerprint does not match a fingerprint stored in memory, the user may only access specific, non-secure menu options on the pocket vault, such as 'Try Again,' 'Pocket Vault Return Information,' 'Emergency Information,' or 'End Session.'" Pet. 41–42 (citing Ex. 1006, 29:31–30:25, 33:5–35:15, Fig. 7). Petitioner asserts that a person of ordinary skill had reason "to incorporate Burger's teachings of preventing user input prior to biometric authorization into the system[s] of Maes and Pare, which already use biometric authorization, at least to help prevent unauthorized attempts to access a user's data and further enhance security." *Id.* at 42 (citing Ex. 1009 ¶ 63). Patent Owner makes no arguments relevant to these claims beyond those discussed above for claim 1. *See* PO Resp. 59.

We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 6 would have been obvious to a person of ordinary skill in the art over Maes, Pare, and Burger, for the reasons given by Petitioner.

b. Claims 7–9

Claim 7 depends from claim 6 and recites that "the secret information known to the user includes a PIN, and wherein the authentication of both the secret information and the biometric input activate the electronic ID device for a financial transaction." Claim 8 depends from claim 7 and recites that "a memory coupled to the processor, wherein data stored in the memory is unavailable to an individual in possession of the electronic ID device until the electronic ID device is activated." Claim 9 depends from claim 8 and recites that "the data is subject to a mathematical operation that acts to modify the data such that it is unintelligible until the electronic ID device is activated." Petitioner maps the limitations of claims 7–9 onto Maes's teachings. Pet. 42–44 (citing Ex. 1003, 3:53–61 (claim 7), 11:9–40 (claim 8), 5:14–17 (claim 9)). Patent Owner makes no arguments relevant to these claims beyond those discussed above for claim 1. *See* PO Resp. 59.

We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 7–9 would have been obvious to a person of ordinary skill in the art over Maes, Pare, and Burger, for the reasons given by Petitioner.

c. Claim 18

Claim 18 depends from claim 16 and recites "de-activating the electronic ID device without generating the encrypted authentication information if the identity of the user is not successfully authenticated to the electronic ID device." Petitioner relies on its assertions regarding claim 1 and asserts further that a person of ordinary skill in the art had reason to "incorporate Burger's teaching of deactivating a device by ending a session or wiping its memory if a user is not successfully authenticated in order to

prevent attackers from gaining access to the device, as taught in Burger." Pet. 46–47 (citing Ex. 1006, 33:27–34:2, 30:20–25, Figs. 7, 9; Ex. 1009 ¶ 64). Patent Owner makes no arguments relevant to this claim beyond those discussed above for claim 1. *See* PO Resp. 59.

Burger discloses that if a user's authorization attempt is not successful, the device may erase its secure memory and "other prudent steps may be taken to ensure that an unauthorized user does not access the Pocket Vault's sensitive contents." Ex. 1006, 33:27–34:2; *see also id.* at 30:20–25, Figs. 7, 9. Thus, Burger teaches the additional limitation of claim 18. We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 18 would have been obvious to a person of ordinary skill in the art over Maes, Pare, and Burger, for the reasons given by Petitioner.

5. Maes, Labrou, and Burger

Petitioner also asserts that Burger's teachings, discussed above regarding combination with Maes and Pare, apply equally to the combination of Maes and Labrou. *See* Pet. 41–47 (challenging claims 6–9 and 18); Inst. 21–25. The notable exception is claim 10, for which Petitioner asserts that Labrou teaches the limitations added by claim 10, and therefore only asserts combinations including Labrou against claim 10. Pet. 44–46; Inst. 24.

Patent Owner relies on its arguments regarding the independent claims and, other than for claim 10, does not contest Petitioner's assertions regarding Maes, Labrou, and Burger. PO Resp. 60–63. Patent Owner argues that Labrou does not teach the limitations of claim 10 and that Petitioner

fails to show why a skilled artisan would use Labrou's teachings allegedly relevant to those limitations. *Id.*

Petitioner relies on the same assertions for claims 10 and 19. *See* Pet. 36. Thus, for the same reason discussed above regarding claim 19, we conclude that Petitioner has not shown the subject matter of claim 10 would have been obvious over Maes, Labrou, and Burger. *See supra* at 41–41.

For the remainder of the claims against which Petitioner asserts a combination of Maes, Labrou, and Burger, Petitioner's arguments are the same as for Maes, Pare, and Burger. Pet. 41–47. Thus, for the reasons discussed above regarding these claims in light of Maes, Pare, and Burger, we conclude Petitioner has shown that the subject matter of claims 6–9 and 18 would have been obvious over Maes, Labrou, and Burger. *See supra* at 43–46.

6. Maes, Pare, Burger, and Labrou

As a result of the way Petitioner asserts the teachings of Pare and Labrou, we determined in the Institution Decision that Petitioner had challenged claim 10 based on a combination of Maes, Pare, Burger, and Labrou. Inst. 24. But Petitioner's assertions against the limitations added by claim 10 depend only on Labrou's disclosures. Pet. 45–46. Thus, we reach the same conclusion for this ground as we have for the challenges based on (1) Maes, Pare, and Burger, and (2) Maes, Labrou, and Burger. *See supra* at 41–41.

We conclude Petitioner has not shown that the subject matter of claim 10 would have been obvious over Maes, Pare, Burger, and Labrou.

7. Pizarro and Pare

Petitioner asserts Pizarro is prior art under 35 U.S.C. § 102(e) based on its October 19, 2004, filing date. Pet. 47. Pizarro discloses a system for using a wireless device to perform transactions. Ex. 1007, Abstract. Pizarro discloses sending biometric information read using the wireless device to a host system, which can confirm the biometric information is consistent with stored information. *Id.* at 2:42–54, 4:3–13, 8:18–27. In some cases, Pizarro discloses verifying identity of a user before allowing use of the device. *Id.* at 9:25–34. Pizarro discloses sending biometric information and account information in an encrypted format to a host system of a financial institution, either directly or through a point-of-sale device. *Id.* at 9:25–55. Pizarro's host system "determines whether to authorize the transaction" including possibly "by verifying the identity of the customer with a remote biometric comparison." *Id.* at 9:56–60.

a. Claim 1

Petitioner maps claim 1's limitations to the references, applying Pizarro as the primary reference that teaches most of the claim limitations. *See* Pet. 49–60. Although Petitioner asserts that Pare also teaches certain limitations, we construe the ground as relying principally on Pizarro as discussed below.

(1) [Preamble] An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction

Petitioner asserts Pizarro teaches the preamble. Pet. 49 (citing Ex. 1007, 2:20–22, 9:18–28). Patent Owner does not contest Petitioner's

assertions in this regard. We conclude Petitioner has shown Pizarro teaches the preamble for the reasons provided by Petitioner.

(2) [a] a biometric sensor configured to receive a biometric input provided by the user

Petitioner asserts Pizarro teaches the claimed biometric sensor. Pet. 49–50 (citing Ex. 1007, 7:35–40, 3:9–21, 4:3–5, 8:18–22, 7:19–40, Fig. 3B). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(3) [b] a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts

Regarding the requirement for the user interface to "receive a user input including secret information known to the user," Petitioner asserts that although Pizarro does not disclose the user entering secret information, Pare teaches requiring a user PIN as part of the authentication process and that a person of ordinary skill had reason to use Pare's teaching "to add an extra layer of security to the authentication process." Pet. 51–52 (citing Ex. 1004, 1:65–2:2, 4:18–24, 4:34–38, 8:36–46, 10:59–61; Ex. 1009 ¶¶ 34, 69). Petitioner further supports the combination with Pizarro's teaching that a customer may establish a "'private key' that may be combined with other data to create a unique, one-time encryption key to minimize the risk of attacks on confidential transaction data." *Id.* (citing Ex. 1007, 8:36–46). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(4) [c] a communication interface configured to communicate with a secure registry

Regarding the requirement to communicate with a "secure registry," Petitioner asserts that the language reads on sending messages to a "host system of a financial institution" in Pizarro. *Id.* at 52–53 (citing Ex. 1007, 5:50–6:1; 2:25–51, 4:32–35, 6:52–65, 7:11–15, 6:35–42, Figs. 3A–B). Petitioner asserts that Pizarro's financial-institution host systems are a secure registry. *Id.* at 53 (citing Ex. 1007, 5:56–6:7, 8:18–28, 9:56–60). Although Pizarro does not appear to expressly recite a "database," it discloses that the host systems use cryptographic protocols to prevent unauthorized access (Ex. 1007, 6:4–7), and that they allow financial institutions to verify customer biometric information received with a particular request against such information stored for each customer (Ex. 1007, 7:59–63, 8:18–28, 9:56–60). We find that Pizarro's financial-institution host systems teach the claimed secure registry.

Petitioner maps the secure registry also to Pare's "Data Processing Center," which uses a database to store information and to confirm that "BIA devices are used only by their rightful owners, to provide financial account information for financial credit and debit transactions, and to allow identification of all BIAs owned by a specific buyer or organization." Pet. 53–54 (quoting Ex. 1004, 49:38–44; citing *id.* at 65:22–29). Petitioner asserts that a person of ordinary skill had reason to use Pare's "Data Processing Center" and "Apparatus Owner Database" with Pizarro's system "to allow information for multiple institutions to be stored in one place." *Id.* (citing Ex. 1009 ¶¶ 41, 71; Ex. 1007, 9:52–55). As we noted in the Institution Decision, Petitioner's assertions in this regard raise alternative

grounds—one applying Pizarro's host system as the secure registry and the other applying Pare's DPC and AOD as the secure registry. Inst. 27–28. Patent Owner does not specifically address this aspect of Petitioner's challenge. *See* PO Resp. 64–68. For the reasons given by Petitioner, we find that Pare's DPC and AOD teach the claimed secure registry.

(5) [d] a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface

Petitioner asserts Pizarro teaches the claimed processor. Pet. 54–55 (citing Ex. 1007, 6:52–7:44, Fig. 3B). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(6) [d][i] the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information

Petitioner asserts Pizarro teaches the claimed programming. Pet. 56 (citing Ex. 1007, 9:25–34, 2:64–3:17). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(7) [d][ii] the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information

Regarding the requirement that the processor be "configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information," Petitioner

asserts a person of ordinary skill would have incorporated Pare's encryption using a nonpredictable value to encrypt a user's biometric input and PIN for transmission. Pet. 57–58 (citing Ex. 1009 ¶¶ 70–71; Ex. 1004, 17:28–47, 18:51–61). Petitioner asserts that using Pare's techniques would add "an additional layer of security to Pizarro's system." *Id.* at 58.

Patent Owner argues that Pizarro does not disclose the user device receiving secret information as an input to generate encrypted authentication information. PO Resp. 65. But Petitioner relies on Pare's disclosure of that limitation, as described above, so Patent Owner's argument is inapposite.

Patent Owner argues that Pare teaches away from combination with another reference that uses tokens (as Patent Owner characters Pizarro) to conduct financial transactions. *Id.* Patent Owner relies on its arguments regarding Maes and Pare (*id.*) and our finding above therefore applies here also—that Pare does not teach away from using its teachings in combination with devices that store information locally. *See supra* at 14–16.

Patent Owner argues that skilled artisans would consider the local-and-remote authentication resulting from combining Pizarro's and Pare's teachings as "redundant and wasteful processing" and that such an approach "would render the device less secure by needlessly exposing the biometric information to fraud during the transmission process." PO Resp. 65–66. According to Patent Owner, Pizarro teaches authenticating biometric information either locally or remotely but not both. *Id.* at 66. Thus, even under Patent Owner's view, Pizarro does not indicate that remote authorization is a security risk. We discuss above why we do not agree with Patent Owner that the redundant nature of local-and-remote authorization

indicates skilled artisans would not have made the asserted combination (*see supra* at 16–18) and we reach the same finding here.

Finally, Patent Owner argues that Petitioner fails to provide an adequate reason that skilled artisans would have combined Pizarro's and Pare's teachings as asserted. PO Resp. 67–68. Because Pizarro discloses an embodiment of local authentication and one of remote authorization, and does not suggest combining those embodiments, Patent Owner asserts Petitioner improperly mixes from the two embodiments. *Id.* Patent Owner's argument, however, ignores that Petitioner asserts a combination incorporating Pare's teachings regarding the use of remote authentication. *See* Pet. 57–58. Once a skilled artisan made the decision to use Pare's teachings regarding remote authorization, that decision to add an additional layer of security by using local-and-remote authorization would have led the skilled artisan to consider Pizarro's teachings regarding remote authorization. Thus, we do not agree with Patent Owner that Petitioner impermissibly relies on both aspects of Pizarro.

Accordingly, we conclude Petitioner has shown Pare teaches this limitation and that skilled artisans would have had reason with rational underpinning to incorporate Pare's teaching with Pizarro's system for the reasons provided by Petitioner.

(8) [d][iii] [processor is configured . . .] to communicate the encrypted authentication information via the communication interface to the secure registry

Petitioner asserts Pizarro teaches the claimed processor configuration for communication. Pet. 58 (citing Ex. 1007, 9:25–39, 9:48–52). Patent Owner does not contest Petitioner's assertions in this regard. We conclude

Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(9) [e][i] wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and

Petitioner asserts Pizarro teaches the claimed transmission configuration for the interface. Pet. 59 (citing Ex. 1007, 9:40–44, 9:34–37, 3:32–59, 4:5–12, 5:52–55, 7:11–20, Fig. 4B). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(10) [e][ii] wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device

Petitioner asserts Pizarro teaches the claimed configuration of the secure registry. Pet. 59–60 (citing Ex. 1007, 9:40–48, 9:56–60; 3:26–59, 4:5–12, 5:52–66, Fig. 4B). Patent Owner does not contest Petitioner's assertions in this regard. We conclude Petitioner has shown Pizarro teaches this limitation for the reasons provided by Petitioner.

(11) Conclusion

Petitioner has shown by a preponderance of the evidence that the combination of Pizarro and Pare teaches the limitations of claim 1 and that skilled artisans would have had reason with rational underpinning to combine Pizarro's and Pare's teachings as asserted. Patent Owner's arguments against those findings are not persuasive. We conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claim 1 would have been obvious to a person of ordinary skill in the art over Pizarro and Pare.

b. Claims 16 and 24

Petitioner maps the limitations of independent claims 16 and 24 to Pizarro and Pare as it does those of claim 1. Pet. 61–65. Patent Owner does not raise arguments specific to claims 16 or 24. PO Resp. 64–68. For the reasons discussed above regarding claim 1, and for the reasons presented in the Petition, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 16 and 24 would have been obvious to a person of ordinary skill in the art over Pizarro and Pare.

c. Claims 2, 5, 11, 13, and 17

Petitioner maps the limitations of claims 2, 5, 11, 13, and 17 onto Pizarro's teachings. Pet. 60–63 (citing Ex. 1007, 7:67–8:3 (claim 2), 6:52–55 (claim 5), 9:30–34 (same), 7:26–35 (claim 11), 9:17–28 (claims 13 and 17)). For those dependent claims, Patent Owner relies on its arguments regarding claim 1. PO Resp. 64–68. We have reviewed Petitioner's contentions and determine that Petitioner has shown by a preponderance of the evidence that the subject matter of claims 2, 5, 11, 13, and 17 would have been obvious to a person of ordinary skill in the art over Pizarro and Pare, for the reasons given by Petitioner.

D. CONTINGENT MOTION TO AMEND

Patent Owner filed a motion to amend the claims, contingent on a determination that any claim is unpatentable. Paper 26 ("MTA"). The motion proposes substitute independent claims 27, 42, and 50, which Patent Owner proposes to take the place of claims 1, 16, and 24, respectively. Proposed substitute claims 27 and 50 modify the respective claims on which they are based by adding features recited in claim 10. MTA 2. Proposed

substitute claim 42 modifies claim 16 by adding limitations similar to those recited in claim 9. *Compare* MTA 8, *with* MTA 9–10.

Regarding the contingent nature of Patent Owner's motion, the motion states "should any of claims 1-3 and 5-26 be determined to be unpatentable, PO respectfully requests that the Board grant this contingent motion such that the '813 Patent be amended to include the substitute claim(s) 1-26." MTA 12. Although that statement could be read as requesting substitution of all proposed claims if any single original claim is determined to be unpatentable, Patent Owner and Petitioner both indicated during the hearing that they viewed the motion as having a one-to-one contingency, such that we should consider a proposed substitute claim only if we determine the corresponding original claim is unpatentable. Tr. 46:12–20, 54:22–55:11. Thus, while we consider Patent Owner's statement in the Contingent Motion to Amend as insufficiently precise, we will proceed based on the parties' collective understanding expressed during the hearing. *Cf. Lectrosonics, Inc. v. Zaxcom, Inc.*, Case IPR2018-01129, slip op. at 3 (PTAB Feb. 25, 2019) (Paper 15) (precedential) ("[A] proposed substitute claim normally will be considered only if a preponderance of the evidence establishes that the original patent claim that it replaces is unpatentable. A patent owner should adopt a claim-by-claim approach to specifying the contingency of substitution, e.g., which claim is to be substituted for which claim, and under what circumstances.").

Therefore, because claim 4 was not challenged in this proceeding (and therefore not determined unpatentable), and because we have determined that Petitioner has not shown any of claims 10, 12, 19, and 21 unpatentable,

we do not consider Patent Owner's motion as to the substitutes for those claims. We consider the motion as to substitutes for claims 1–3, 5–9, 11, 13–18, 20, and 22–26 (proposed claims 27–29, 31–35, 37, 39–44, 46, and 48–52, respectively). "[T]he Board determines whether substitute claims are unpatentable by a preponderance of the evidence based on the entirety of the record, including any opposition made by the petitioner." *Lectrosonics*, slip op. at 4.

1. Requirements of 35 U.S.C. § 316(d) and 37 C.F.R. § 42.121

A motion to amend must propose a reasonable number of substitute claims. 35 U.S.C. § 316(d)(1)(B); 37 C.F.R. § 42.121(a)(3). Because Patent Owner proposes one substitute claim for each current claim, it proposes a reasonable number of substitute claims. *See* 37 C.F.R. § 42.121(a)(3).

Proposed substitute claims must respond to a ground of unpatentability involved in the trial. 37 C.F.R. § 42.121(a)(2)(i). Patent Owner contends that the limitations added by proposed substitute claims 27, 42, and 50 are not taught by the references asserted by Petitioner. MTA 4–5.

Proposed substitute claims may not enlarge the scope of the claims. 35 U.S.C. § 316(d)(3); 37 C.F.R. § 41.121(a)(2)(ii). Patent Owner's proposed change—incorporating limitations either in, or similar to those in, existing dependent claims—does not enlarge the scope of the claims. Additionally, as Patent Owner points out, although proposed substitute claim 36 omits limitations that appear in claim 10, which claim 36 would replace, those limitations were included in proposed substitute claim 27, from which claim 36 would depend. MTA 2–3.

A motion to amend must show that the limitations of the proposed substitute claims have written-description support in the specification. 37 C.F.R. § 42.121(b)(1). Patent Owner provides a chart of proposed substitute claims that includes citations for written-description support to the as-filed application.[13] MTA 6–12 (citing Ex. 1002, 810:28–811:13 (Ex. 1001, 46:46–47:6) (regarding limitations added in proposed claims 27 and 50), 809:1–5 (Ex. 1001, 45:28–35) (regarding limitations added in proposed claim 42), 809:8–12 (Ex. 1001, 45:40–47) (same), 816:17–19 (Ex. 1001, 50:47–49) (same)).

2. Proposed Claims 27 and 50 and dependents

Proposed claim 27 would amend claim 1 to further recite:

> wherein the processor is further configured to generate a seed using at least two of an electronic serial number, a discrete code associated with the electronic ID device, a PIN, a time value, and the biometric input to generate the encrypted authentication information, the seed being employed by the processor to generate the non-predictable value.

MTA 6–7. Proposed claim 50 recites limitations parallel to those of proposed claim 27 but in method form. *Id.* at 11. Petitioner raises several arguments that claims 27 and 50 would have been obvious.

a. Maes and Labrou

Petitioner contends that proposed claims 27 and 50 would have been obvious over Maes and Labrou. MTA Opp. 2–5. It additionally contends

[13] As discussed below, depending on the construction of the proposed amended claim, we do not agree with Patent Owner that the Specification provides adequate written-description support for the proposed claim. *See infra* at 62.

proposed claims 28–31, 37–41, 51, and 52 would have been obvious over the same two references. *See id.* at 2, 8. Addressing the limitation added to claim 1 by proposed claim 27, Petitioner argues that Labrou discloses generating a seed, S′, used to generate the RSN (which Petitioner asserts is the nonpredictable value). MTA Opp. 3; *see supra* at 32. In particular, Petitioner argues that Labrou teaches generating the seed with (1) a discrete code associated with the electronic ID device and (2) a time value. MTA Opp. 3–4; Tr. 23:11–15.

Labrou teaches generating a pseudorandom number using a seed, S, and function, R, that are stored on each device. Ex. 1005 ¶ 527 ("The RSN is a pseudorandom number that is generated from a locally stored pseudorandom sequence number function R (a pseudorandom number generator). . . . Typically the generation of a pseudorandom number also involves another parameter, a seed S. . . . Each AP device has its own R and S, which are securely stored on the device and at the AVP."). Additionally, Labrou teaches using a time value to generate a new seed for the RSN generator. *Id.* ¶ 536 ("If desired, as the base time advances, the seed may also be updated. For example, the new seed S′ may be the S′=R (S, T_0′, T_0) where S is the original seed, T_0 is the original base time, and T_0[′] is the new base time."); *see also id.* ¶¶ 506 ("Agreement Parties, AP1 (1101) and AP2 (1102)" and "Authentication and Verification Party AVP"), 528 ("Timestamp (TS): The time associated with a transaction.").

Petitioner argues that skilled artisans had reason to use Labrou's teachings discussed above because such pseudorandom number generator functions "were commonly used for encryption by 2006" and "necessarily

required a seed input." MTA Opp. 4. Further, explains Petitioner, "it was well known to include a dynamic value, such as the time value taught in Labrou, as part of the input for generating a seed . . . to create entropy for the non-predictable value, thus enhancing its non-predictability and the security of the encryption based thereon." *Id.* (citing Ex. 1022 ¶¶ 7–8, 22).

(1) generating a seed using . . . a discrete code associated with the electronic ID device

Patent Owner challenges whether Labrou's seed S is "a discrete code associated with the electronic ID device." MTA Reply 4. According to Patent Owner, that term means "a value associated with the device that is subject to change." *Id.* at 3–5. Patent Owner relies on a statement in the Specification that the "discrete code may be maintained by the user device," allowing the device to set the code to a default value upon compromised security. *Id.* at 3–4 (quoting Ex. 1001, 47:8–15). Patent Owner's argument, however, ignores the Specification's description of multiple embodiments for the discrete code, which do not all indicate the discrete code is subject to change. *See* Ex. 1001, 47:1–8; MTA Surreply 2. Thus, we do not agree that the claimed "discrete code associated with the electronic ID device" must be subject to change.

Patent Owner offers no other argument regarding Labrou's disclosures asserted against the additional limitation of proposed claims 27 and 50. For the reasons discussed above and in Petitioner's Opposition to the Motion to Amend, we agree with Petitioner that Labrou teaches the additional limitations of proposed claims 27 and 50.

(2) Whether Petitioner justifies combining Labrou and Maes

Patent Owner challenges Petitioner's assertions, first arguing that Petitioner fails to identify exactly how Maes would be modified by the combination with Labrou. MTA Reply 5. The challenge, however, follows Petitioner's challenge to claim 1 based on Labrou and Maes (*see* MTA Opp. 2), and we have discussed how Maes's and Labrou's teachings fit together as explained in the Petition (*see supra* at 31–36). Labrou's teachings relevant to the additional limitation of proposed claims 27 and 50 relate to a particular method for determining the nonpredictable value (*see* Ex. 1005 ¶¶ 527, 536), which is already part of claim 1, as discussed above. Thus, we agree with Petitioner that skilled artisans would have had reason to generate Labrou's pseudorandom number according to Labrou's own teachings, especially because including the time value when generating the number would have enhanced nonpredictability and therefore security. *See* MTA Opp. 4.

(3) Conclusion

For the reasons discussed above regarding claim 1 and the additional reasons discussed regarding proposed claims 27 and 50, we conclude Petitioner has shown by a preponderance of the evidence that proposed claims 27 and 50 would have been obvious to persons of ordinary skill in the art over Maes and Labrou.

Proposed claims 28–41 depend from proposed claim 27 and proposed claims 51 and 52 depend from proposed claim 50. *See* MTA 7–9, 11–12. As discussed above, we do not consider the contingent motion as to proposed claims 30, 36, or 38. *See supra* at 56. As to proposed claims 28, 29, 31–35, 37, 39–41, 51, and 52, Patent Owner offers no independent arguments for

the patentability of the respective proposed claims. *See* MTA Reply 1–9. Each dependent proposed claim mirrors the language of an existing claim. We determine above that Petitioner has shown the limitations added by dependent claims 2, 3, 5, 11, 13–15, 17, 20, 22, 23, 25, and 26 do not render those claims patentably distinct over Maes and Labrou. *See supra* at 37–41. Thus, Petitioner has also shown proposed claims 28, 29, 31, 37, 39–41, 51, and 52 unpatentable over Maes and Labrou, for the reasons discussed above.

b. Maes, Labrou, and Gullman

Petitioner contends that proposed claims 27–29, 31, 37, 39–41, and 50–52 would have been obvious over Maes, Labrou, and Gullman[14]. MTA Opp. 10–13.

Gullman discloses a method for authorizing access in which a token is generated and forwarded to a host that decodes the token back to the information it contains. Ex. 1023, 1:32–37. Gullman's "token is a non-predictable code derived from a private key, e.g. a unique fixed value, and a public key, e.g. a time varying value." *Id.* Because the token is nonpredictable and uses a time-varying input, it provides security during transmission. *Id.* at 1:38–45. Gullman discloses using biometric information "as part of the 'seed' for generating the token." *Id.* at 2:20–23. In particular, "[t]he verification algorithm uses the template data, the biometric input, a fixed code (i.e., PIN, embedded serial number, account number) and time varying self-generated information to derive a token output." *Id.* at 2:55–59. The biometric input is used by comparing it to a stored template to determine a correlation factor indicating how well the input matches the

[14] U.S. Patent No. 5,280,527, issued January 18, 1994 (Ex. 1023).

template. *Id.* at 6:16–20. The correlation factor is used with the other information to derive a token. *Id.* at 6:30–34. Once that token is transmitted to a host, the host "decrypts or decodes the token to derive the fixed code and correlation factor." *Id.* at 6:37–39.

Addressing the limitation added to claim 1 by proposed claim 27, Petitioner argues that Gullman teaches "methods for using a biometric measurement as part of the 'seed' for generating a non-predictable security token (i.e., 'non-predictable value')." MTA Opp. 11 (citing Ex. 1023, 2:20–26, 1:32–34). Petitioner further argues that Gullman's method uses a time-varying code, such as the time of day, in combination with the biometric inputs and a fixed code such as a PIN, to generate its token. *Id.* (citing Ex. 1023, 2:53–59, 4:3–8).

Petitioner submits that a skilled artisan had reason to combine Gullman's method with Maes's and Labrou's teachings to create a seed for a nonpredictable value: it would have provided the "benefit of enhancing the strength of the non-predictable security token (and thus enhancing security) from combining multiple different values, including time and other values unavailable to outsiders, such as a PIN, an electronic serial number, and/or biometric information) as the seed." *Id.* at 12 (citing Ex. 1022 ¶ 27).

(1) Whether Gullman teaches generating a seed using multiple inputs

Patent Owner challenges Petitioner's assertions, arguing that Gullman does not disclose using a fixed code and time-varying information to generate a seed, but rather uses biometric information to generate a seed, then uses that seed in combination with other information to generate a token. MTA Reply 14–15. Patent Owner's argument contradicts both the Specification and Gullman's disclosures.

The portion of the Specification upon which Patent Owner relies for written-description support for the added limitation states that, "in one embodiment, the seed is employed in an algorithm that also employs a temporal value to generate the authentication information." Ex. 1002, 810:30–811:31 (Ex. 1001, 46:53–55); *see* MTA 6. The portion that Patent Owner relies on for written-description support does not discuss a "time value" in any other regard. Ex. 1002, 810:28–811:13 (Ex. 1001, 46:46–47:6); *see* MTA 6; *see also* Ex. 1001, 46:46–50 ("[A]ny two of the PIN, the biometric information, the electronic serial number, a discrete code associated with the device and the identifying information concerning the selected account are employed to generate a seed."; not including a "time value" as an input to generate a seed). Thus, under Patent Owner's construction where the limitation added to proposed claims 27 and 50 requires a time value to be used to generate the seed itself, those claims lack written-description support in the Specification. Alternatively, if the Specification provides support for proposed claims 27 and 50, then the claims encompass a situation where a time value is used in combination with a seed to generate a nonpredictable value—just as Patent Owner describes Gullman's operation. *See* MTA Reply 14–15.

But beyond the written-description problem that Patent Owner's argument raises, the argument misconstrues Gullman's disclosures. Gullman states that "biometric information is used as part of the 'seed' for generating the token." Ex. 1023, 2:22–23; *see also* Ex. 1022 ¶¶ 26–28. Thus, we find that Gullman discloses the limitation added in claims 27 and 50.

(2) Whether Gullman discloses an operable method

Patent Owner argues that skilled artisans would not have used Gullman's teachings because Gullman's process "would simply not work." MTA Reply 16–17. According to Patent Owner, a person of ordinary skill in the art would not understand from the disclosures how Gullman's host could determine the correlation factor once receiving the token. *Id.* Like its argument regarding Labrou (*see supra* at 33), however, Patent Owner's argument relates to enablement of the prior art and therefore does not overcome an assertion of obviousness. *See ABT Sys.*, 797 F.3d at 1360 n.2. Labrou's plain disclosures indicate that the host decodes a token to recover the correlation factor (Ex. 1023, 6:37–39), and, as discussed above, those disclosures provide a basis for Petitioner's obviousness ground.

(3) Conclusion

For the reasons discussed above regarding claim 1 and the additional reasons discussed regarding proposed claims 27 and 50, we conclude Petitioner has shown by a preponderance of the evidence that proposed claims 27 and 50 would have been obvious to persons of ordinary skill in the art over Maes, Labrou, and Gullman. As discussed above, Petitioner has shown that dependent claims 2, 3, 5, 11, 13–15, 25, and 26 would have been obvious over Maes and Labrou (*see supra* at 37–41) and, therefore, for the same reasons discussed above, Petitioner has shown proposed dependent claims 28, 29, 31, 37, 39–41, 51, and 52 would have been obvious over Maes, Labrou, and Gullman.

c. Maes, Labrou, and Burger, and Maes, Labrou, Gullman, and Burger

Petitioner contends that proposed dependent claims 32–35 would have been obvious over Maes, Labrou, and Burger, for the same reasons as for dependent claims 6–9 and 11. MTA Opp. 8–9. Petitioner also contends that the same claims would have been obvious over Maes, Labrou, Gullman, and Burger for the same reasons. *Id.* at 19–20. Patent Owner offers no independent arguments for the patentability of those claims. *See* MTA Reply 1–9, 12–17. Because each claim mirrors the language of an existing claim, for the reasons discussed above, Petitioner has shown by a preponderance of the evidence that the subject matter of proposed claims 32–35 would have been obvious over Maes, Labrou, and Burger, and also over Maes, Labrou, Gullman, and Burger. *See supra* at 43 (claims 6–9 and 18).

3. Proposed Claim 42 and dependents

Proposed claim 42 would amend claim 16 to further recite:

> wherein data stored in the electronic ID device is subject to a mathematical operation employing the secret information that acts to modify the data such that it is unintelligible until the electronic ID device is activated, and the electronic ID device uses the secret information to reverse the mathematical operation and render the data legible.

MTA 10. Petitioner raises several arguments that proposed claim 42 would have been obvious.

a. Maes and Labrou

Petitioner contends proposed claim 42 would have been obvious over Maes and Labrou. MTA Opp. 5–8. It additionally contends proposed

claims 43–49 would have been obvious over the same two references. *See id.* at 2, 8.

(1) Maes's teaching

Addressing the limitation added to claim 16 by proposed claim 42, Petitioner points out that Maes teaches data on the user's local device is encrypted before being stored in memory and decrypted when accessed, and that information such as a PIN must be entered to activate the device and access the data. MTA Opp. 6–7 (citing Ex. 1003, 3:59–64, 5:14–17, 7:51–56, 11:27–32). Petitioner argues that it would have been obvious to skilled artisans to perform Maes's local-data "encryption using a basic XOR ('exclusive-OR') operation with a secret string, such as a keyword or password, as one of the simplest, most computationally inexpensive means to reversibly render data on a device unintelligible." *Id.* at 6–7 (citing Ex. 1022 ¶¶ 9, 10, 12). Petitioner relies in part on Maes disclosing its invention may "employ any known encryption technique or algorithm" and referencing a book that explains XOR operations. *Id.* (quoting Ex. 1003, 10:11–14).

Patent Owner argues that Maes already states that data on the customer's device is "decrypted by the encryption/decryption module 24 using an encryption key unique to the PDA device 10" and submits that Petitioner provides no reason to change that to a different method. MTA Reply 10 (quoting Ex. 1003, 11:29–32). We do not agree with Patent Owner. Although Maes teaches a method of encryption, that does not undermine Petitioner's reasoning that a skilled artisan would have had reason to use the known method of an XOR operation with a secret string because it had the benefit of being computationally inexpensive. *See* Ex. 1022 ¶ 10. Thus, we

conclude that Petitioner has shown that performing the step added by proposed claim 42 to secure data on the electronic ID device would have been obvious in light of Mae's teachings.

(2) Labrou's teaching

Petitioner argues alternatively that Labrou teaches its PIE, which may include a PIN, "may be used in an XOR operation for performing encryption to reversibly render the RSN unintelligible." MTA Opp. 6–7 (citing Ex. 1005 ¶¶ 537–538). Petitioner reasons that using those teachings would have been obvious because "[s]imple XOR encryption operations that use a string (such as a PIN) as a key to encrypt and decrypt have long been a well-known encryption technique that provided a benefit of being computationally inexpensive." *Id.* (citing Ex. 1022 ¶¶ 10, 23).

Patent Owner challenges these assertions, and argues that Labrou, when using an XOR operation to generate an encryption key, additionally uses a hash function to generate the key as its output, and therefore does not produce a reversible result. MTA Reply 11–12 (citing Ex. 1005 ¶¶ 537–538). Petitioner responds that it never proposed using a hash function following the XOR operation in the asserted combination. MTA Surreply 6. According to Petitioner, the reason a skilled artisan would have used the XOR operation was because of computational simplicity, which justifies using the XOR operation alone. *See id.*

We agree with Petitioner. Although Labrou discloses a more complex arrangement using a hash function to generate an encryption key, Petitioner has justified why a person of ordinary skill would have had reason to use simply the XOR operation that Labrou discloses. Patent Owner does not explain why a skilled artisan reading Labrou's teachings would incorporate

all aspects of Labrou's method, particularly when Patent Owner asserts that doing so would not have worked for on-device encryption using a user's PIN. *See* MTA Reply 12.

Accordingly, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of proposed claim 42 would have been obvious over Maes and Labrou. For proposed dependent claims 43, 44, 46, 48, and 49, Petitioner asserts that the additional subject matter added by those claims would have been obvious for the same reasons as dependent claims 17, 18, 20, 22, and 23, respectively. MTA Opp. 8. Patent Owner offers no independent arguments for the patentability of those claims. *See* MTA Reply 9–12. Thus, for the reasons discussed above regarding claims 17, 18, 20, 22, and 23, we conclude that the subject matter of proposed claims 43, 44, 46, 48, and 49 would have been obvious over Maes and Labrou. *See supra* at 39–41.

b. Maes, Labrou, and Burger

Petitioner contends that proposed dependent claim 44 would have been obvious over Maes, Labrou, and Burger, for the same reasons as for dependent claim 18. MTA Opp. 9. Patent Owner offers no independent arguments for the patentability of claim 44. *See* MTA Reply 1–9. Because claim 44 mirrors the language of existing claim 18, for the reasons discussed above, Petitioner has shown by a preponderance of the evidence that the subject matter of claim 44 would have been obvious over Maes, Labrou, and Burger. *See supra* at 45.

c. Maes, Labrou, and Weiss

Petitioner contends that proposed claim 42 would have been obvious over Maes, Labrou, and Weiss[15]. MTA Opp. 16–18. According to Petitioner, Weiss discloses using an XOR operation with a password to encrypt data stored on a device. *Id.* at 16–17. Petitioner asserts that skilled artisans had reason to incorporate Weiss's method with Maes because it "was a well-known technique for limiting access to data stored on a device in a computationally inexpensive way." *Id.* at 17 (citing Ex. 1022 ¶¶ 10, 38, 39). Additionally, in light of Maes's statement that its invention "may employ any known encryption technique or algorithm for the encryption/decryption process," Petitioner contends that using Weiss's method with Maes would have been straightforward. *Id.*

Patent Owner argues that there was no reason to modify Maes, which already uses an encryption key, and that Petitioner provides no evidence that Maes's method was computationally taxing or had a deficiency. MTA Reply 22–23. Like Patent Owner's similar arguments, which we address above, this argument is not persuasive because Petitioner does not need to show that Maes lacked a particular functionality, only that there was a reason to use the teaching from another reference. Particularly where, as here, Petitioner asserts that a combination would provide a particular benefit—computational simplicity—that sufficiently justifies its proposed combination. *See* MTA Surreply 9.

Thus, we conclude that Petitioner has shown that performing the step added by proposed claim 42 to secure data on the electronic ID device would

[15] U.S. Patent No. 5,479,512, issued December 26, 1995 (Ex. 1025).

have been obvious in light of Weiss's teachings, and has thus shown by a preponderance of the evidence that the claim would have been obvious over Maes, Labrou, and Weiss. *See supra* at 32–37 (addressing unpatentability of claims 1 and 16 over Maes and Labrou).

d. Maes, Labrou, Weiss, and Burger

Petitioner submits that the additional limitation of proposed claim 44 would have been obvious over Burger for the same reasons as claim 18, which shares claim language with proposed claim 44. MTA Opp. 20 (citing Ex. 1022 ¶ 45). Patent Owner does not appear to address these contentions other than challenging the conclusion as to claim 1 and proposed claim 42. *See generally* MTA Reply.

For the reasons discussed above regarding proposed claim 42 and claim 18, we conclude that Petitioner has shown by a preponderance of the evidence that the subject matter of proposed claim 44 would have been obvious to a person of ordinary skill in light of Maes, Labrou, Weiss, and Burger.

4. Additional arguments by Petitioner

Petitioner argues also that proposed claims 27 and 50 would have been obvious over a combination of Maes, Labrou, and Jakobsson,[16] applying Jakobsson much as it applies Gullman in the ground discussed above. MTA Opp. 13–16. In light of our conclusions above that the proposed claims are not patentable over multiple combinations of prior art, we do not reach this additional combination.

[16] U.S. Patent Application Publication No. 2004/0172535, published September 2, 2004 (Ex. 1024).

Petitioner also argues that the proposed substitute claims fail to recite patent-eligible subject matter under 35 U.S.C. § 101. *Id.* at 20–25. In light of our conclusions above that the proposed claims are not patentable over the prior art of record, we do not reach this additional argument.

E. REAL PARTY IN INTEREST

A petition must identify all real parties in interest ("RPIs"). 35 U.S.C. § 312(a)(2). The petitioner bears the burden of persuasion to show that it accurately names all RPIs. *Applications in Internet Time, LLC v. RPX Corp.*, 897 F.3d 1336, 1343 (Fed. Cir. 2018) ("*AIT*") (citing *Zerto, Inc. v. EMC Corp.*, Case IPR2014-01295, slip op. at 6–7 (PTAB Mar. 3, 2015) (Paper 34)). We generally accept a petitioner's initial identification of its RPIs unless the patent owner presents some evidence to support its argument that an unnamed party should be included as an RPI. *Worlds Inc. v. Bungie, Inc.*, 903 F.3d 1237, 1242 (Fed. Cir. 2018).

The Petition identifies Unified Patents, Inc. ("Unified"), as the sole RPI in this proceeding. Pet. 67. Patent Owner argues that Petitioner should have named [redacted] as a real party in interest (RPI) and that, therefore, we should dismiss the Petition. PO Resp. 68–70. According to Patent Owner, our prior decisions that have found Unified was the only RPI focused too heavily on which party controlled the IPR. *Id.* at 69. Patent Owner argues that approach is incorrect in light of *AIT*. *Id.*

Patent Owner's argument that [redacted] is an unnamed RPI appears to be based on several assertions. Patent Owner asserts that "Unified is a for-profit company seeking to 'mitigate NPE risk for its members[]' by filing IPRs." *Id.* at 70 (emphasis omitted) (quoting Ex. 2007 (Unified 2014 website);

citing Ex. 2008 (Unified 2016 website); Ex. 2009 (Unified 2013 website); Ex. 2010 (Brief of Amici Curiae Unified Patents) ("Unified provides a valuable service to its members" (emphasis omitted))). Patent Owner asserts that this IPR "was filed in response to [redacted]" for Unified to file IPRs on its behalf. PO Resp. 70 (citing Ex. 2011 (Membership Agreement); Ex. 2012 [redacted]).

Petitioner, on the other hand, contests Patent Owner's assertions and points to record evidence that "Unified solely directed, controlled, and funded this challenge." Reply 20 (citing Ex. 1036 ¶ 5 (Declaration of Kevin Jakel)). Petitioner states that it "had no pre-filing communications with [redacted] or any other Unified member regarding this IPR, the '813 Patent, any litigation involving it, or [Patent Owner]." *Id.* (citing Ex. 1036 ¶ 3; Ex. 1037, 123:12–13 (Jakel deposition)). Regarding the membership fees, Petitioner contends, with support from its CEO, that they "are not designated to be used to file challenges, much less any particular challenge." *Id.* (citing Ex. 1036 ¶¶ 7, 12). And Petitioner submits that it directs its activities in so-called "zones," or technology sectors, and that the zone relevant to the '813 patent has 128 members. *Id.* (citing Ex. 1036 ¶ 8). Further, Petitioner points out that [redacted] to the '813 patent (CBM2018-00024, -00025, and -00026). *Id.* at 20–21.

Additionally, Petitioner distinguishes *AIT* because the parties involved in that case had prefiling discussions and the petitioner in that case held itself out as "an extension of a client's in-house legal team" and shared a common director with the client at issue. Reply 22 (quoting *AIT*, 897 F.3d at

1340–41). We note and agree with those factual distinctions between the case at hand and *AIT*. More significantly, the alleged unnamed RPI in that case would have been barred from filing a petition because of the § 315(b) time bar. *AIT*, 897 F.3d at 1338–39. Patent Owner does not allege that [redacted] would have been time barred here, so this proceeding does not implicate § 315(b). *Cf. Ventex Co., Ltd. v. Columbia Sportswear N. Am., Inc.*, Case IPR2017-00651 (Jan. 24, 2019) (Paper 152) (precedential).

Whether a particular entity is a real party in interest is a "highly fact-dependent question" that is assessed "on a case-by-case basis." Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,759 (Aug. 14, 2012) ("TPG"). We consider multiple factors, including: whether a non-party is funding, directing, or controlling the IPR; whether the non-party had the ability to exercise control; the non-party's relationship with the petitioner and with the petition, including any involvement in the filing; and the nature of the entity filing the petition. TPG, 77 Fed. Reg. at 48759–60.

Patent Owner's contentions are not persuasive. It raises at most general statements that membership in Unified will benefit a company by reducing patent-litigation risk. *See* Ex. 2007, 2008, 2009, 2010. As relates to [redacted], Patent Owner raises no evidence of a specific interest in this proceeding other than that [redacted]. PO Resp. 70. Indeed, although Patent Owner asserts this proceeding "was filed in response to [redacted]," it does not cite any evidence to support that assertion other than that [redacted] is a member of Unified. *Id.* Similarly, when Patent Owner asserts that "Unified has no independent interest in invalidating the '813 patent, and attempts to do so for

[redacted]" (*id.* at 71), it does not cite any evidence. Patent Owner did not seek to compel discovery on this issue.

Against Patent Owner's assertions, Petitioner offers evidence that there was no connection between [redacted] and this proceeding. Reply 20–21 (citing Ex. 1036 ¶ 5–8; Ex. 1037, 123:12–13, 160:10–162:9, 163:12–164:17). We determine that Petitioner's evidence, as described above, supports that the Petition was not filed at the behest of [redacted]. *See* TPG, 77 Fed. Reg. at 48,759. Thus, as possible support for Patent Owner's argument, we are left with Unified's business model and that [redacted]. We conclude that [redacted] is insufficient to show [redacted] is an RPI here, in light of specific evidence showing no connection between [redacted] and this proceeding and the fact that [redacted] We further conclude that the evidence of record does not establish that all members of Unified are RPIs merely by fact of their membership. *See* TPG, 77 Fed. Reg. at 48,760. As to that conclusion, we are in accord with the conclusion of multiple other Board decisions on the issue. *See, e.g.*, *Unified Patents, Inc. v. Uniloc 2017 LLC*, Case IPR2017-02148 (PTAB April 11, 2019) (Paper 74).

Accordingly, we conclude that Petitioner has not failed to name all real parties in interest.

III. CONCLUSION

For the foregoing reasons, we determine that Petitioner has shown by a preponderance of the evidence that: (1) each of claims 1–3, 5, 11, 16, 20, and 24 is unpatentable over Maes and Pare; (2) each of claims 1–3, 5, 11, 13–17, 20, and 22–26 is unpatentable over Maes and Labrou; (3) each of

claims 13–15, 17, 20, 22, 23, 25, and 26 is unpatentable over Maes, Pare, and Labrou; (4) each of claims 6–9 and 18 is unpatentable over Maes, Pare, and Burger; (5) each of claims 6–9 and 18 is unpatentable over Maes, Labrou, and Burger; and (6) each of claims 1, 2, 5, 11, 13, 16, 17, and 24 is unpatentable over Pizarro and Pare.

Petitioner has not shown by a preponderance of the evidence that: (1) any of claims 13–15, 17, 22, 23, 25, and 26 is unpatentable over Maes and Pare; (2) any of claims 12, 19, and 21 is unpatentable over Maes and Labrou; (3) any of claims 12, 19, and 21 is unpatentable over Maes, Pare, and Labrou; (4) claim 10 is unpatentable over Maes Labrou, and Burger; or (5) claim 10 is unpatentable over Maes, Pare, Burge, and Labrou.

Petitioner has shown by a preponderance of the evidence that Patent Owner's proposed substitute claims are not patentable. In particular, Petitioner has shown by a preponderance of the evidence that: (1) each of proposed claims 27–29, 31, 37, 39–44, 46, and 48–52 is unpatentable over Maes and Labrou; (2) each of proposed claims 27–29, 31, 37, 39–41, and 50–52 is unpatentable over Maes, Labrou, and Gullman; (3) each of proposed claims 32–35 and 44 is unpatentable over Maes, Labrou, and Burger; (4) each of proposed claims 32–35 is unpatentable over Maes, Labrou, Gullman, and Burger; (5) each of proposed claims 42, 43, 46, 48, and 49 is unpatentable over Maes, Labrou, and Weiss; and (6) proposed claim 44 is unpatentable over Maes, Labrou, Weiss, and Burger.

IV. ORDER

Accordingly, it is:

ORDERED that claims 1–3, 5–9, 11, 13–18, 20, and 22–26 of the '813 patent are unpatentable;

FURTHER ORDERED that claims 10, 12, 19, and 21 of the '813 patent have not been proven unpatentable;

FURTHER ORDERED that Patent Owner's Contingent Motion to Amend is denied; 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. § 90.2.

PETITIONER:

Jason Mudd
jason.mudd@eriseip.com

Roshan Mansinghani
roshan@unifiedpatents.com

Eric Buresh
eric.buresh@eriseip.com

Jonathan Stroud
jonathan@unifiedpatents.com

PATENT OWNER:

Jim Glass
jimglass@quinnemanuel.com

Tigran Guledjian
tigranguledjian@quinnemanuel.com

Christopher Mathews
chrismathews@quinnemanuel.com

Nima Hefazi
nimahefazi@quinnemanuel.com