Trials@uspto.gov
571-272-7822

Paper 43
Entered: September 8, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PNC BANK, N.A., U.S. BANK, N. A., U.S. BANCORP, BANK OF THE WEST, SANTANDER BANK, N.A.; ALLY FINANCIAL, INC.; RAYMOND JAMES & ASSOCIATES, INC.; TRUSTMARK NATIONAL BANK; NATIONWIDE BANK; SYNCHRONY BANK; GENERAL ELECTRIC COMPANY; COMMERCE BANK; and CADENCE BANK, N.A.,
Petitioner,

v.

SECURE AXCESS, LLC,
Patent Owner.

Case CBM2014-00100[1]
Patent 7,631,191 B2

Before BARBARA A. BENOIT, TRENTON A. WARD, and GEORGIANNA W. BRADEN, *Administrative Patent Judges*.

BENOIT, *Administrative Patent Judge*.

---

[1] Case CBM2015-00009 has been consolidated with the instant proceeding.

FINAL WRITTEN DECISION
35 U.S.C. § 328(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

This is a covered business method ("CBM") patent case, under § 18 of the Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284, 331 (2011).[2] We have jurisdiction to hear this review under 35 U.S.C. § 6(c). For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–32 of U.S. Patent No. 7,631,191 B2 (Ex. 1001; "the '191 patent") are unpatentable.

This Final Written Decision is issued pursuant to 35 U.S.C. § 328(a) and 37 C.F.R. § 42.73. This Final Written Decision is entered concurrently with a final written decision in *EMC Corp. v. Secure Axcess, LLC*, Case IPR2014-00475, an *inter partes* review of claims 1–23 and 25–32 of the '191 patent.

A. Procedural History

PNC Bank, N.A. ("PNC"), U.S. Bank, N.A., and U.S. Bancorp (together, "U.S. Bank"; collectively with PNC, "Petitioner") filed a Petition (Paper 3; "Pet.") requesting a covered business method patent review of claims 1–32 (the "challenged claims") of the '191 patent. Patent Owner, Secure Axcess, LLC, filed a Preliminary Response opposing institution of a review. Paper 7. On September 9, 2014, pursuant to 35 U.S.C. § 324(a), we instituted a covered business method patent review for claims 1–32 of the

[2] *See GTNX, Inc. v. INTTRA, Inc.*, 789 F.3d 1309, 1310 (Fed. Cir. 2015) (describing transitional program for review of covered business method patent under 35 U.S.C. §§ 321–329, pursuant to the AIA).

'191 patent as unpatentable under 35 U.S.C. § 103(a) over SHTTP[3] and Arent.[4] Paper 10 ("Inst. Dec.") 34–35.

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 21; "PO Resp."), and Petitioner filed a Reply (Paper 22; "Reply"). Patent Owner filed observations on the cross-examination of Petitioner's declarant (Paper 30), to which Petitioner filed a response (Paper 37). Patent Owner also filed a Motion to Exclude certain evidence. Paper 31 ("Mot."). Petitioner filed an Opposition (Paper 36; "Pet. Opp."), and Patent Owner filed a Reply (Paper 39; "PO Reply").

An oral hearing was held on May 20, 2015. Paper 42 ("Hearing Tr.").

B. Related Matters

Petitioner represents that the '191 patent has been asserted against PNC in *Secure Axcess, LLC v. PNC Bank, N.A.*, Case No. 6:13-cv-00722-LED (E.D. Tex.) and has been asserted against U.S. Bank in *Secure Axcess, LLC v. U.S. Bank, N.A.*, Case No. 6:13-cv-00717-LED (E.D. Tex.). Pet. 2, Paper 6. Petitioner also identifies sixteen other court proceedings in which Patent Owner has asserted the '191 patent. *See* Pet. 2-3; *see also* Paper 6 (Patent Owner's Related Matters).

In addition to *PNC Bank, N.A. v. Secure Axcess, LLC*, Case CBM2014-00100, the '191 patent has been the subject of petitions for

---

[3] E. RESCORLA & A. SCHIFFMAN, *The Secure HyperText Transfer Protocol*, the Internet Engineering Task Force (July 1996) (Ex. 1009; "SHTTP" or "the SHTTP document").

[4] U.S. Patent No. 6,018,724, issued Jan. 25, 2000, filed June 30, 1997 (Ex. 1003; "Arent").

covered business method patent reviews brought by other petitioners. In *Bank of the West v. Secure Axcess, LLC*, Case CBM2015-00009, the Board instituted review of claims 1–32 and then consolidated that review with this review. *Bank of the West v. Secure Axcess, LLC*, Case CBM2015-00009 (PTAB April 13, 2015; Paper 21) (PTAB May 12, 2015; Paper 27).

The Board further instituted, on June 22, 2015, a covered business method patent review of claims 1–5, 16, and 29–32 of the '191 patent brought by yet another petitioner. *See T. Rowe Price Inv. Servs, Inc. v. Secure Axcess, LLC*, Case CBM2015-00027 (PTAB June 22, 2015; Paper 9). On July 10, 2015, the Board denied institution of a second petition by PNC seeking another covered business method patent review of the '191 patent. *See PNC Bank, N.A. v. Secure Axcess, LLC*, Case CBM2015-00039 (PTAB July 10, 2015; Paper 9).

C. The '191 Patent

The '191 patent relates to authenticating data, such as a web page. Ex. 1001, Abstract, 1:16–18; 12:9–18 (claim 1). The '191 patent explains that customers can be deceived by web pages that appear to be authentic but are not. *See id.* at 1:28–34. A web page that has been authenticated according to the techniques described by the '191 patent includes "all of the information in the same format as the non-authenticated page." *Id.* at 2:58–60. The authenticated web page, however, also includes an "authenticity stamp." *Id.* at 2:60–62.

Figures 1 and 2 are set forth below:

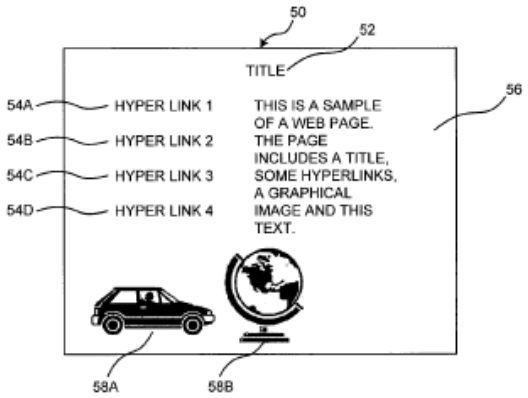

Figure 1

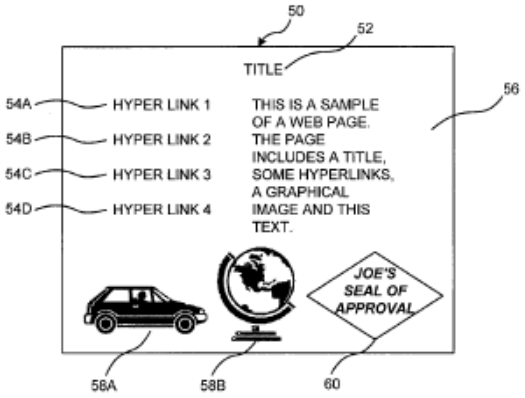

Figure 2

Figures 1 and 2 each show web page 50 having title 52, hyperlinks 54A, 54B, 54C, and 54D, textual information 56, and graphical images 58A and 58B. *Id.* at 2:54–57. Figure 1 shows web page 50 has not been authenticated, whereas Figure 2 shows web page 50 has been authenticated. *Id.* at 2:54–61. The authenticated web page shown in Figure 2, unlike the non-authenticated web page shown in Figure 1, includes authenticity stamp 60. *Id.*

The '191 patent discloses an exemplary environment using an authentication server. *Id.* at Abstract; *see id.* at 3:26–55, Fig. 4. In that embodiment, a web server at a web site receives a request for information from user's web browser and, prior to sending the requested web page to the user's computer, the web server submits information to an authentication server. *Id.* at 3:41–51. The authentication server adds authentication information to the request for information. *Id.* at 3:50–53. "The information which includes the authentication information is returned to the web server[,] which then sends the web page including the authentication

information to the user [computer]." *Id.* at 3:52–55. The '191 patent also describes combining the logic of an authentication server with the logic of a web server. *Id.* at 4:57–58.

The '191 patent further discloses that an authentication server is not always necessary. *Id.* at 8:17–18 ("In alternative embodiments, there is no authentication server."). In such an embodiment, for example, a web server receives a request for a web page. *Id.* at 4:5–14. "If the [web] page is to be authenticated, the page is dynamically signed with a private key and additional information. . . ." *Id.* at 4:14–16. The signed web page then is returned to the user's computer, and the user's computer verifies the authenticity of the web page, using a public key to verify the digital signature. *Id.* at 4:18–23. After verification of the digital signature, the user computer "can validate the authentication of the [web] page." *Id.* at 4:23–24.

D. Illustrative Claims of the '191 Patent

Claims 1, 17, 29, 31, and 32 of the '191 patent are independent and generally relate to methods, authentication systems, and a computer-readable medium for inserting an authenticity key into formatted data (claim 17) or to create formatted data (claims 1, 31, 32), and sending (or returning) formatted data having an authenticity key (claims 1, 29, 31). Claims 1 and 17, reproduced below, are illustrative of the claimed subject matter:

> 1. A method comprising:
>
> transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data; and

> returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file,
>
> wherein an authenticity stamp is retrieved from the preferences file.
>
> 17. An authentication system comprising:
>
> an authentication processor configured to insert an authenticity key into formatted data to enable authentication of the authenticity key to verify a source of the formatted data and to retrieve an authenticity stamp from a preferences file.

Ex. 1001, 12:9–18, 12:62–67.

II. DISCUSSION

A. Covered Business Method Patent

AIA section 18 establishes a post-grant review proceeding "for review of the validity of covered business method patents." § 18(a)(a). The statute defines a "covered business method patent" as "a patent that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service . . . ." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). Congress provided a specific exception to this definition of a covered business method patent—"the term does not include patents for technological inventions." *Id.*

As a threshold matter in considering whether to institute a review, the Board determined, after considering the Petition and Patent Owner's Preliminary Response (Paper 7), that the '191 patent is a covered business

method patent and is eligible for a covered business method patent review. Inst. Dec. 13–18; *see* AIA § 18(a)(1)(E) ("[t]he Director may institute a transitional proceeding [under § 18] only for a patent that is a covered business method patent."). During the covered business method patent review, Patent Owner again contested whether the '191 patent is a covered business method patent. PO Resp. 23–41.

1. Financial Product or Service

First, Patent Owner contends the '191 patent is ineligible for covered business method patent review because its invention is not directed to a financial product or service and can be used by institutions other than financial institutions. PO Resp. 27–34. Specifically, Patent Owner contends that covered "financial products and services" include "only financial products such as credit, loans, real estate transactions, check cashing and processing, financial services and instruments, and securities and investment products." PO Resp. 25.

The reasoning of Patent Owner's contention was rejected during rule-making and, more recently, by the Federal Circuit. During rule-making, the Office stated:

> The suggestion to clarify that the term "financial product or service" is limited to the products or services of the financial services industry is not adopted. Such a narrow construction of the term would limit the scope of the definition of covered business method patents beyond the intent of section 18(d)(1) of the AIA.

77 Fed. Reg. 48,734 , 48,736 (Aug. 14, 2012). The Federal Circuit recently affirmed the Office's position: "We agree with the USPTO that, as a matter

of statutory construction, the definition of 'covered business method patent' is not limited to products and services of only the financial industry, or to patents . . . directly affecting the activities of financial institutions such as banks and brokerage houses." *Versata Dev. Grp., Inc. v. SAP Am., Inc.*, 2015 WL 4113722 at *16 (Fed. Cir. July 9, 2015). As the court points out, "[t]he plain text of the statutory definition contained in § 18(d)(1)—'performing . . . operations used in the practice, administration, or management of a financial product or service'—on its face covers a wide range of finance-related activities." *Id.*

The method and apparatus claimed by the '191 patent perform operations used in the practice, administration, or management of a financial product or service and are incidental to a financial activity. The written description of the '191 patent discloses a need by financial institutions to ensure customers are confident that the financial institution's web page is authentic (Ex. 1001, 1:28–33). Additionally, the '191 patent discloses alternative embodiments of the invention as being used by financial institutions (*id.* at 8:21–23, 11:23–40, 11:52–67).

The '191 patent relates to authenticating a web page and claims a particular manner of doing so. Ex. 1001, 1:16–18, 12:9–18. The '191 patent is directed to solving problems related to providing a web site to customers of financial institutions. Thus, the '191 patent covers the ancillary activity related to a financial product or service of Web site management and functionality and so, according to the legislative history of the AIA, the

method and apparatus of the '191 patent perform operations used in the administration of a financial product or service.

We recognize that the legislative history of the AIA has "competing statements from various legislators with regard to the possible scope of [these] issues." *Versata Dev. Grp.*, 2015 WL 4113722 at *12. We note nonetheless that at least one legislator viewed "customer interfaces" and "Web site management and functionality," which are at issue here, as ancillary activities intended to be encompassed by the language "practice, administration and management" of a financial product or service. 157 Cong. Rec. S1364–65 (daily ed. Mar. 8, 2011) (statement of Sen. Schumer) (indicating the language "practice, administration and management" of a financial product or service "is intended to cover any ancillary activities related to a financial product or service, including, without limitation, marketing, customer interfaces, Web site management and functionality, transmission or management of data, servicing, underwriting, customer communications, and back office operations—e.g., payment processing, stock clearing").

Although not determinative, Patent Owner's allegations of infringement of claims of the '191 patent by approximately fifty financial institutions is a factor weighing toward the conclusion that the '191 patent claims a method or apparatus that at least is incidental to a financial activity, even if other types of companies also practice the claimed invention. *See* Pet. 12 (representing Patent Owner has sued approximately fifty financial institutions).

We have considered whether the Board's determination that the '191 patent claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service should be changed in light of the Patent Owner's Response. *See* Inst. Dec. 15; AIA § 18(d)(1); 37 C.F.R. § 42.301(a). For the foregoing reasons, we maintain our determination.

2. Exclusion for Technological Inventions

The definition of "covered business method patent" in section 18 of the AIA expressly excludes patents for "technological inventions." AIA § 18(d)(1); *see* 37 C.F.R. § 42.301(a). To determine whether a patent is for a technological invention, we consider "whether the claimed subject matter as a whole recites a technological feature that is novel and unobvious over the prior art; and solves a technical problem using a technical solution." 37 C.F.R. § 42.301(b).

The Office published a notice identifying examples of certain claim drafting techniques that typically would not render an invention a "technological invention." Office Patent Trial Practice Guide, 77 Fed. Reg. 48,756, 48,764 (Aug. 14, 2012). These are:

> (a) Mere recitation of known technologies, such as computer hardware, communication or computer networks, software, memory, computer-readable storage medium, scanners, display devices or databases, or specialized machines, such as an ATM or point of sale device.
>
> (b) Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious.

> (c) Combining prior art structures to achieve the normal, expected, or predictable result of that combination.

Id.

The Board concluded at institution that the '191 patent was not for a technological invention. Inst. Dec. 15–18. Patent Owner also contends that the '191 patent is not eligible for covered business method patent review because the invention of the '191 patent is "for a machine that implements a technological solution." PO Resp. 34 (initial capitalization removed); *see id.* at 34–41.

Specifically, Patent Owner contends the claims of the '191 patent solve the technical problem of distinguishing authentic data for web pages from fraudulent data sent by a fraudulent web site. PO Resp. 34–35. Patent Owner contends that the claimed subject matter as a whole provides a technological solution—a computer-implemented system that includes a processor, an authenticity stamp, and an authenticity key organized into a specific structure, function and operation—that is novel and nonobvious. *Id.* at 35–39.

We consider whether the claimed subject matter as a whole has a technological feature that solves a technical problem using a technical solution. *See Versata Dev. Grp.*, 2015 WL 4113722 at *17 (putting aside the regulation's definition of novel and nonobvious because "presumably the invention under review, since it has already been covered by an issued patent, was earlier determined by the USPTO to be novel and nonobvious" and analyzing whether the patent was for a technological invention based on

whether the patent has a technological feature that solves a technical problem using a technical solution).

Neither the problem addressed nor the solution that solves the problem addressed by the '191 patent is technological. As Patent Owner acknowledges, the problem addressed is distinguishing authentic web pages sent by a legitimate web site from fraudulent web pages sent by a fraudulent site. *See* PO Resp. 34. To solve the problem that users have difficulty distinguishing authentic from non-authentic web pages, the invention as a whole displays an icon or other "authenticity stamp" to indicate to the user that the web site is authentic. *See* Ex. 1001, Abstract ("The present invention provides for an icon with an additional level of functionality that allows a user to validate that current information (e.g., a web page) originates from the true owner. . . ."), 2:58–60, Figs. 1, 2 (disclosing that a web page that has been authenticated according to the techniques described by the '191 patent includes "all of the information in the same format as the non-authenticated page" and also includes an "authenticity stamp."), 12:9–14:31 (all claims require retrieving an authenticity stamp from a preferences file); *see also* PO Resp. 2 (describing the problem of fraudulent web pages from an Internet user's point of view).

Displaying an authenticity stamp to indicate to the user that the web site is authentic is not a technological solution. This is indicated by the functional nature of the claims. For instance, some claims require "verifying authenticity . . . based on the authenticity key" or "validating [a web page] based on the authenticity key," without specifying the technical operations to

be used to verify or validate other than the general statement "based on the authenticity key." Ex. 1001, 12: 23–25 (claim 3), 12:48–51 (claim 13).

A feature of the solution is an "authenticity key." The technological features for the authenticity key are not recited by the claims. Rather, the claims recite how the authenticity key is used—inserting an authenticity key or a second authenticity key into data or data having an authenticity key (independent claims 1, 17, 29, 31, 32; dependent claims 13, 23), receiving an authenticity key from a third party (claim 11), verifying or validating data based on an authenticity key (claims 3, 13), displaying data in response to the verification of the authenticity key (claim 4).

Moreover, the '191 patent discloses using cryptographic techniques to generate the authenticity key and verify authenticity, without specifying cryptographic algorithms for encryption and decryption. *See id.* at 6:28–32. Instead, the '191 patent incorporates by reference a cryptography text (*id.* at 10:44-48), which further undermines Patent Owner's contention that the invention of the '191 patent has a technological feature that solves a technical problem using a technical solution. *See Versata Dev. Grp.*, 2015 WL 4113722 at *17 (citing 77 Fed. Reg. at 48,764) (explaining that the Office Trial Practice Guide indicates mere "recitation of known technologies," "reciting the use of known prior art technology," and "combining prior art structures to achieve the normal, expected, or predictable result of that combination" do not help support a finding that the invention is within the technological invention exception).

The independent claims recite that the authenticity stamp is retrieved from a preferences file and dependent claims 5 and 6 further recite the authenticity stamp is displayed for certain data. *Id.* at 12:17–18 (claim 1), 12:29–32 (claims 5 and 6), 12:66–67 (claim 17), 14:9–10 (claim 29), 14:21–22 (claim 31), 14:31 (claim 32). Further, the '191 patent describes an authenticity stamp as having a number of variations, including graphics only, text only, text and graphics, audio, blinking (Ex. 1001, 2:67–3:7), but does not describe novel or nonobvious technology used to implement those features.

Moreover, Patent Owner's contention that subject matter of the invention solves a technological problem using a technical solution is undermined by disclosures of the '191 patent indicating the components of the computer system are known technologies. *See Versata Dev. Grp.*, 2015 WL 4113722 at *17 (citing 77 Fed. Reg. at 48,764) (explaining that the Office Trial Practice Guide indicates mere "recitation of known technologies," "reciting the use of known prior art technology," and "combining prior art structures to achieve the normal, expected, or predictable result of that combination" do not help support a finding that the invention is within the technological invention exception). For example, the '191 patent discloses known computer systems and devices running known operating systems (Ex. 1001, 3:30–34, 10:30–35, 11:7–12), known user input devices (*id.* at 11:3–6), and known networks and networking and communication protocols (*id.* at 3:38-44, 10:67–11:3, 11:12–17). The '191 patent further discloses that the system is programmed using known

programming and scripting languages, and known data structures (*id.* at 10:35–40), and discloses that the system uses "conventional techniques for data transmission, signaling, data processing, network control, and the like" (*id.* at 10:41–44).

We are not persuaded that the claimed subject matter, as a whole, requires any specific, unconventional software, computer equipment, cryptography algorithms, processing capabilities, or other technological features. Furthermore, Patent Owner's identification of allegedly novel or unobvious steps, such as limitations in the independent claim and dependent claims 2 and 4 (PO Resp. 36), does not persuade us that any of the steps require the use of specific computer hardware alleged to be novel and unobvious over the prior art. Reciting the use of known prior art technology to accomplish a process or method, even if that process or method is novel and non-obvious does not render the claimed subject matter a technological invention. *See* 77 Fed. Reg. at 48,764.

Having considered Patent Owner's Response, we maintain the determination that the '191 patent is not a technological invention.

3. Eligible for Covered Business Method Patent Review

Having determined that the '191 patent claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service and does not fall within the exception for technological inventions, we maintain our determination that the '191 patent is eligible for a covered business method patent review.

B. Claim Construction

In a covered business method patent review, a claim in an unexpired patent shall be given its broadest reasonable construction, in light of the specification of the patent in which it appears. 37 C.F.R. § 42.300(b); *cf. In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1278, 1279 (Fed. Cir. 2015) (regarding a similar broadest reasonable construction standard for an *inter partes* review, the court held "Congress implicitly approved the broadest reasonable interpretation standard in enacting the AIA," and "the standard was properly adopted by PTO regulation."), *reh'g en banc denied*, 793 F.3d 1297 (Fed. Cir. 2015). Under that standard, claim terms are presumed to be given their ordinary and customary meaning as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Any special definition for a claim term must be set forth in the specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). A particular embodiment appearing in the written description should not be read into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993). We construe the terms below and discuss terms relative to prior art disclosures in accordance with these principles.

The parties each propose constructions for various claim terms and oppose several of one another's proposed constructions. We address disputed terms as necessary for this decision.

The parties also refer to claim constructions from prior litigation involving the '191 patent. Pet. 15–19; PO Resp. 14–19; *see also* Ex. 2002 (Mem. Op. and Order, *Secure Axcess, LLC v. Bank of Am. Corp.*, No. 6:10-cv-00670 (E.D. Tex. July 9, 2012, ECF No. 461) ("Markman Order"). We apply a different claim construction standard than that applied by a district court, and are not generally bound by a judicial construction of a claim term. *Power Integrations, Inc. v. Lee*, No. 2014-1123, 2015 WL 4757642, at *6 (Fed. Cir. Aug. 12, 2015). Nonetheless, we are mindful of the judicial constructions of the terms "authenticity key," "preferences file," and "authenticity stamp." Markman Order 21. Those terms, however, need not be construed expressly for this decision, so we need not determine whether those constructions are consistent with the broadest reasonable construction of the terms. *Cf. Power Integrations*, 2015 WL 4757642, *7 ("We do not hold that the board must in all cases assess a previous judicial interpretation of a disputed claim term.").

1. "Received Data"

Independent claims 1, 31, and 32 recite "received data."[5] Patent Owner proposes, with support of its declarant Jonathan Katz, Ph.D., that "transforming, at an authentication host computer, received data" (recited in independent claim 1), "instructions to format received data by inserting an

[5] The court determined that no construction was necessary for "received data." Markman Order 13–14. The court also rejected both Patent Owner's proposed construction of "data indicative of at least part of a web page" and the defendants' proposed construction of "a webpage or other document requested by the user." *Id.*

authenticity key to create formatted data" (recited in independent claim 31), and "the authentication host computer receives the data to create received data" (recited in independent claim 32) require the authentication host computer "to receive data from outside of itself." PO Resp. 8–9; Ex. 2006 ¶¶ 19, 24.

As made clear by Patent Owner's arguments concerning prior art references, Patent Owner further proposes that each of independent claims 1, 31, and 32, which recite "received data," be construed additionally to require data sent from a device. PO Resp. 43–44 (arguing prior art is insufficient because it discloses "the same server that creates a document, also signs the document"). Petitioner opposes construing "received data" and the limitations which recite "received data" as data sent from another device ("outside of itself") because the '191 patent discloses an embodiment in which the logic of the authentication server and the logic of the web server is combined on the same server. Reply 2 (citing Ex. 1001, 8:17–19); *see* Ex. 1001, 4:57–58 ("the logic of the authentication server may be combined with the logic of the web server"). Petitioner's declarant Paul C. Clark, D. Sc. supports Petitioner's position. Ex. 1017 ¶ 4 (citing Ex. 1001, 4:57–58, 8:17–19).

As an initial matter, in accordance with the plain language of the claims and because the '191 patent does not provide any special meaning for the term "received data," we construe "received data" to mean "data that has been received." The term "received data" implies data has been received but does not itself require the data to be received at a particular time, in a

particular manner, by a particular device (such as an authentication host computer), or from a particular device (such as a device other than an authentication host computer).

None of independent claims 1, 31, or 32 expressly recites from where the received data is sent, much less recites expressly that the data is sent from a device other than the authentication host computer. Of independent claims 1, 31, and 32, only independent claim 32 expressly requires a particular device—"an authentication host computer"—to receive data. Independent claims 1 and 31 require acting on received data in a certain manner—to transform (claim 1), or format (claim 31), received data in a certain manner to create formatted data. Thus, none of claims 1, 31, or 32 expressly requires an authentication host computer to receive data from a device other than the authentication host computer, as Patent Owner contends.

In reciting "transforming, at an authentication host computer, received data," independent claim 1 requires the transforming be performed by a particular device—"an authentication host computer." In reciting "received data," claim 1 impliedly requires data have been received but does not require the data to be received by a particular device, such as an authentication host computer.

This construction is consistent with the '191 patent because claim 1 recites "an authentication host computer," a term that does not appear in the '191 patent other than in the claims and does not recite "an authentication

server," a term that does appear in the written description of the '191 patent.[6] Because the '191 patent discloses embodiments that do not require an authentication server, we will not equate the claim term "authentication host computer" with the disclosed authentication server. *See* Ex. 1001, 4:5–43, Fig. 5 (using a web server that digitally signs without involving a separate authentication server), *id.* at 4:57–58 (describing a combined web server and authentication server). This view is confirmed by the prosecution history of the '191 patent. *See Microsoft Corp. v. Proxyconn, Inc.*, 789 F.3d 1292, 1298 (Fed. Cir. 2015) ("The PTO should also consult the patent's prosecution history in proceedings in which the patent has been brought back to the agency for a second review."). The applicants during examination deliberately removed "authentication server" from a pending claim. Ex. 1005, 112 (deleting "authentication server" from application claim 8 in response to the Office action dated July 16, 2008). Later to address a rejection that the claim did not recite patent-eligible subject matter, the applicants added "an authentication host computer"—not "authentication server"—to claim 1. *Id.* at 93 (adding "authentication host computer" to application claim 1 in response to the Office action dated January 9, 2009).

Additionally, during examination, the applicants removed from claim 1 a limitation specifying a source from which the data was received

---

[6] Patent Owner apparently equates the recited "authentication host computer" with the "authentication server" disclosed in the '191 patent. *See, e.g.*, PO Resp. 9–13 (relying on an "authentication server" depicted in Ex. 1001, Figs. 9, 10 for support of Patent Owner's contention that the recited "authentication host computer" receives data from a web server).

and then deleting the receiving step entirely. *Id.* at 165 (changing "receiving data *from* a client" to "receiving data *for* a client" in claim 1 in response to the Office action dated October 18, 2007), 111 (deleting "receiving data for a client to create received data" in application claim 1 in response to the Office action dated July 16, 2008).

Thus, the applicants deliberately broadened claim 1 by removing a limitation specifying from where the data is received. This further confirms our determination that the transformation limitation in claim 1 should not be construed to require the authentication host computer to receive data from outside of itself or from another device (such as a client computer or a web server), which is a more narrow construction than the plain language of the claim requires.

We turn to independent claim 31, which does not require an authentication host computer. Patent Owner contends that independent claim 31 requires an authentication host computer to receive data outside of itself and further requires the authentication host computer to receive data from another device. PO Resp. 42 ("The combination of [the prior art references] does not teach 'transforming, at an authentication host computer, received data'. . . *as similarly recited in independent claims 31* and 32") (initial capitalization removed; emphasis added).

Independent claim 31 does not recite an "authentication host computer" but rather recites a "computer readable medium having . . . instructions to format received data." We are not persuaded that the recited instructions must be executed by an authentication host computer because

other embodiments are described by the ’191 patent, among them an embodiment using a web server that digitally signs without involving separate authentication server (Ex. 1001, 4:5–43, Fig. 5) and a combined web server and authentication server (*id.* at 4:57–58).

Turning to independent claim 32, the plain language “the authentication host computer receives the data to create received data” requires the authentication host computer to receive data. We are not persuaded, however, that independent claim 32 requires the authentication host computer to receive data from outside of itself or from another device, as Patent Owner contends.

First, we credit Dr. Clark’s testimony (Ex. 1017) supporting Petitioner’s position (Pet. 2) that the authentication host computer need not receive data from outside of itself or from another device. Dr. Clark’s testimony is based on the disclosure of the ’191 patent of an embodiment combining the logic of the authentication server and the web server (Ex. 1001, 4:57–58, 8:17–18).

Neither Patent Owner nor its declarant address persuasively how this disclosure of a combined web server and authentication server (*id.* at 4:57–58) or the use of the term authentication server in the ’191 patent (as opposed to claimed “an authentication host computer”) would affect how one of ordinary skill in the art would understand the scope of independent claim 32.

We, therefore, determine that independent claims 1, 31, or 32 do not require an authentication host computer to receive data from outside of itself or from a device other than the authentication host computer.

2. "Authenticity Key" and "Locating a Preferences File"

Independent claims 1, 29, 31, and 32 each recites some limitation regarding the authenticity key and locating a preferences file. Independent claim 1 recites "returning . . . the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file." Independent claim 29 recites "the authenticity key enables location of a preferences file." Independent claim 31 recites "the authenticity key is retrieved from the formatted data to locate a preferences file." Similarly, independent claim 32 recites "retrieving, by the client computer, the authenticity key from the formatted data to locate a preferences file."

Independent claim 17 does not recite a locating a preferences file but recites retrieving something from a preferences file. Specifically, independent claim 17 recites "an authentication processor configured to insert an authenticity key into formatted data to enable authentication of the authenticity key to verify a source of the formatted data and to retrieve an authenticity stamp from a preferences file."

The parties dispute whether these claims require the preferences file to be hidden and require "the authentication key to provide the ability to determine a location of a preference file," as Patent Owner contends (PO Resp. 19–22). For the following reasons, we do not construe the independent claims 1, 17, 29, 31, and 32 to require the preferences file to be

hidden or to require the authentication key be used to, or provides the ability to, determine a location of a preference file.

Preferences File Need Not Be Hidden

Turning first to whether the claims require the recited "preferences file" to be hidden, Patent Owner contends that all of the challenged claims require the "preferences file" to be hidden—its location not to be known. None of the independent claim recite expressly hiding or obscuring the location of the preferences file, or that the location of the preferences file is hidden or obscured. In support of its position, Patent Owner relies on a preferred embodiment disclosed in the written description in which the location of the preferences file is obscured. *See, e.g.,* PO Resp. 20 (citing Ex. 1001, 4:37–40). Patent Owner's contentions seem to require the location of the preferences file to be concealed, rather than merely not being known. *Id*. at 21, 50.

In response, Petitioner opposes, indicating "to enable the authenticity key . . . to locate a preferences file" and similar claim terms do not require the location of the preferences file to be hidden. Reply 2–3. Petitioner acknowledges that the '191 patent describes the file location of the preferences file as "not readily known to the" user computer. *Id.* at 3 (quoting Ex. 1001, 4:37–38). With support of its declarant, Petitioner contends that, even so, "the location is not hidden to everyone." *Id.* (citing 1017 ¶ 6).

Furthermore, the ’191 patent indicates that “the location of the preferences file is not readily known” to the user computer in an exemplary embodiment.

Petitioner correctly notes that the ’191 patent does not require a preferences file be hidden but only discloses the location may be obscured or not readily known in preferred, but not all, embodiments. Ex. 1001, 4:5–7, 37–40 (indicating in an exemplary embodiment, “the location of the preferences file is not readily known” to the user computer, so the user computer “must get the preferences key to determine the location of the preferences file”). In another example, the ’191 patent indicates that “*[p]referably*, the preferences file is placed in a random directory to help obscure the location of the preferences file.” *Id.* at 9:53–55 (emphasis added). Thus, the ’191 patent does not require a preferences file be hidden but only discloses the location may be obscured or not readily known in preferred, but not all, embodiments.

We decline to read limitations into a claim from these preferred embodiments described in the Specification when the claim language is broader than the embodiment. *In re Am. Acad. of Sci. Tech Ctr*., 367 F.3d 1359, 1364 (Fed. Cir. 2004); *In re Van Geuns*, 988 F.2d at 1184. Here, the claim language is broader than the preferred embodiments describing the location of the preferences file as obscured or not readily known and, therefore, should not be narrowed by embodiments in the ’191 patent. Furthermore, the ’191 patent does not set forth a special definition for that claim term with reasonable clarity, deliberateness, or precision that would

impose a special meaning requiring the location of the preferences file be obscured or hidden. *See In re Paulsen*, 30 F.3d at 1480.

Accordingly, the term "to locate a preferences file" in claims 1, 31, and 32, as well enabling "location of a preferences file" in claim 29, do not require the location of the preferences file be obscured or hidden. Nor does "enabl[ing] authenticiation of the authenticity key . . . to retrieve an authenticity stamp from a preferences file," as recited in independent claim 17, require the preferences file to be obscured or hidden.[7]

Enabling the Authenticity Key to Locate a Preferences File

Petitioner contends that none of the claims require the formatted data or the authenticity key be used to locate the preferences file. Pet. 15–16. Rather, Petitioner contends independent claims 1, 29, 31, and 32 only require "enabling, by an authenticity key as a precondition, a process of determining a preferences file." *Id*. at 16.

Patent Owner does not challenge directly whether the authenticity key must be used to locate the preferences file. Patent Owner, however, contends that the claims require "the authentication key to provide the ability to determine a location of a preference file." PO Resp. 19–20, 50.

We agree with Petitioner that none of the claims require the authenticity key to locate the preferences file or have the ability to determine the location of a preferences file. First, none of the independent claims

[7] Patent Owner includes this limitation of claim 17 in the heading of its argument but does not explain why this particular limitation would require locating a preferences file. PO Resp. 19–22.

recite the authenticity key being used to locate the preferences file. Nor is there evidence of written description support for such an interpretation—the '191 patent does not disclose using an authenticity key to locate the preferences file. Rather, as noted previously, the '191 patent discloses in a preferred embodiment that a preferences key, which is different than an authenticity key, is used to locate the preferences file. *See* Ex. 1001, 4:38–40.

Petitioner's proposed construction of independent claims 1, 29, 31, and 32 as "enabling, by an authenticity key as a precondition, a process of determining a preferences file" better comports with the claims and written description of the '191 patent. Pet. 16. For example, the '191 patent discloses that after verification of a received digital signature, the preferences key is requested and subsequently used to determine the location of the preferences file. *See* Ex. 1001, 4:22–40 (referring to Fig. 5). The verification of the received digital signature must occur before the preferences key can be requested and used to determine the location of the preferences file. In other words, verification of the received digital signature is a precondition of requesting and using the preferences key to determine the location of the preferences file. Thus, verification of the received digital signature enables—supplies the opportunity for[8]—the requested preferences key.

[8] AMERICAN HERITAGE DICTIONARY 605 (3d ed. 1992) (defining "enable" as "1. To supply the means, knowledge, or opportunity; make able") (Ex. 3001).

Thus, we agree with Petitioner that none of the claims require the formatted data or the authenticity key be used to locate the preferences file.

C. Obviousness Over SHTTP and Arent

Petitioner asserts that claims 1–32 of the '191 patent are unpatentable under 35 U.S.C. § 103 over SHTTP and Arent. Pet. 19–71. To support its contentions, Petitioner provides analysis, relying on declaration testimony of Dr. Clark. *Id.* (citing Ex. 1002). Patent Owner responds, relying on declaration testimony of Dr. Katz. PO Resp. 41–79 (citing Ex. 2006).

1. Principles of Law Regarding Obviousness

To prevail in challenging claims 1–32 of the '191 patent, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 326(e); 37 C.F.R. § 42.1(d).

Under 35 U.S.C. § 103(a), a claim is unpatentable if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).
The question of obviousness is resolved on the basis of underlying factual determinations including the following: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

2. Level of Ordinary Skill in the Art

In determining whether an invention would have been obvious at the time it was made, 35 U.S.C. § 103 requires us to determine the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. "The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry." *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991). The person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). The level of ordinary skill in the art is reflected by the prior art of record. *Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001). Factors that may be considered in determining the level of ordinary skill in the art include, but are not limited to, the types of problems encountered in the art, the sophistication of the technology, and educational level of active workers in the field. *Id.* In a given case, one or more factors may predominate. *Id.* Generally, it is easier to establish obviousness under a higher level of ordinary skill in the art. *Innovention Toys, LLC v. MGA Entm't, Inc*., 637 F.3d 1314, 1323 (Fed. Cir. 2011) ("A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse.").

Petitioner's expert adopted the level of ordinary skill in the art at the time of the invention used by Patent Owner's expert. *See* Ex. 2006 ¶ 8 (testimony by Patent Owner's declarant identifying the level of ordinary skill); Ex. 1002 ¶ 29 (testimony by Petitioner's declarant). We do not

disagree with the parties. Therefore, one of ordinary skill in the art would have a bachelor's degree in computer science, computer engineering, or an equivalent field and least two years of work experience in the area of information technology.

3. Priority Date of Claims 1–32

As a threshold matter, we turn to the issue of whether Arent can be asserted in this covered business method patent review. Arent is a patent, which issued from an application filed on June 30, 1997—a date prior to the earliest effective filing date claimed by the '191 patent—September 9, 1999. Thus, on this record, we find Arent is prior art at least under 35 U.S.C. § 102(e) to the challenged claims. Under AIA § 18(a)(1)(C), however, prior art under 35 U.S.C. § 102(e) is not available for consideration in a covered business method patent review.

Petitioner asserts that Arent is prior art under 35 U.S.C. § 102(a) and, as such, is available for consideration in a covered business method patent review. Pet. 21. Petitioner asserts that September 6, 2000 is the earliest date of which the '191 patent is entitled to claim benefit, because the provisional application (Ex. 1007), of which the '191 patent claims benefit, does not provide the requisite support for any of the claims. *Id*. at 19–20. Thus, according to Petitioner, Arent, which issued January 25, 2000, is prior art under 35 U.S.C. § 102(a), because Arent issued before the effective filing date of the '191 patent. *Id*. at 21.

Specifically, Petitioner, with support from its declarant Dr. Clark asserts that the provisional application does not disclose "the combinations

of an 'authenticity key,' 'preferences file,' and 'authenticity stamp' recited in each independent claim. Pet. 20 (citing Ex. 1002 at 18, ¶ 37). Petitioner asserts "[a]t best, the provisional application only generically discloses using a shared secret between a merchant and a consumer for authentication." Pet. 20. Patent Owner does not contest Petitioner's assertions.

The provisional application, on its face, is a "new invention disclosure form" for an invention titled "Enhanced Browser Security System." Ex. 1007, 4. "The invention provides for an icon with an additional level of functionality to allow the consumer to validate the current web page originates from the true owner of the icon (and is not in fact a mere copy)." *Id.* "The invention proposes to utilize the shared secret data created as part of being" a credit card holder of a particular credit card company. *Id.* at 5–6.

We agree with Petitioner and its declarant that the provisional application does not disclose the claimed authenticity key or preferences file or the claimed use thereof, as recited in each of independent claims 1, 17, 29, 31, and 32. The provisional application describes the invention in a few sentences. The scarcity of detail fails to provide sufficient disclosure of the claimed steps.

For example, we see no disclosure of inserting any data in the provisional application, much less inserting something that could be identified as an authenticity key. Although a shared secret is disclosed, the shared secret is not described as being inserted into the web page or any other data. *See id.* at 5–6 ("The invention proposes to utilize the shared secret data created as part of being" a credit card holder of a particular credit

card company.). Moreover, the record evidence indicates that the provisional application does not disclose the recited "authenticity key." Pet. 20 (citing Ex. 1002 at 18, ¶ 37).

Thus, we agree with Petitioner that the provisional application lacks written description support for "authenticity key," which is recited by all claims in the '191 patent. Accordingly, we determine Arent is prior art under 102(a) to the '191 patent and is available for consideration in this covered business method patent review.

4. Summary of the SHTTP Document

Petitioner represents that the SHTTP Document is prior art under 35 U.S.C. §§ 102(a) and 102(b), having been published in July 1996, more than a year prior to the earliest effective filing date claimed by the '191 patent. The SHTTP document is a draft document of the Internet Engineering Task Force ("IETF") describing the Secure HyperText Transfer Protocol ("SHTTP protocol"). Ex. 1009, 1. The SHTTP protocol is a method "for securing messages sent using the HyperText Transfer Protocol ("HTTP"), which, in turn, forms the basis for the World Wide Web." Ex. 1009, 1. Thus, the SHTTP provides secure communication mechanisms between a client computer and a server to enable commercial transactions. Ex. 1009, 2.

According to the SHTTP document, digital signatures may be used in the SHTTP protocol. *See, e.g.*, Ex. 1009, 5 (¶ 1.4.1), 32 (¶ 6.4.3, ¶ 7.1.1). For example, the SHTTP document describes a "digital signature enhancement" in which "an appropriate certificate may . . . be attached to the message." *Id.* at 5 (¶ 1.4.1). Also the SHTTP document describes a

server or third party digitally signing a document to create a signed document, which is cached in the server's storage and later sent to a client computer and used to verify the authenticity of the signed document. *See id.* at 32–33. Petitioner refers to this type of digital signature as "static pre-signing." Reply 5 (citing Ex. 1009, 8–9, 32–33). The SHTTP document also describes "recursive encapsulation" of messages. Ex. 1009, 33. In recursive encapsulation, a signed message, which includes a digital signature attached to a document, becomes "the inner content" of a new SHTTP message. *Id.* at 33–34. Thus, in recursive encapsulation a message includes another message.

The SHTTP document also describes displaying, on the client computer, a visual indicator of the security of the transaction and indicating the identity of the signer of the signed document. *See id.* at 31.

5. Summary of Arent

Arent describes authenticating online transaction data. Ex. 1010, Abstract. A validation process is initiated when a user initiates an electronic transaction, and the validation process "determin[es] authenticity of data related to the transaction, such as the identity of a transaction party." *Id.* If the data are authentic, Arent's process displays a "certification indicator," which may be a graphic with user defined text and may be customized by a user. *Id.*

Arent's Figure 6 is set forth below:

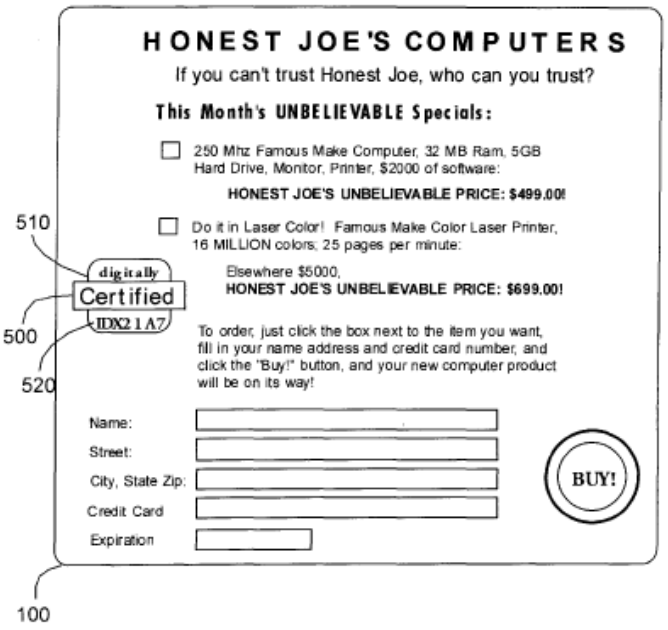

FIG. 6

Figure 6 illustrates an example of certification indicator with a user-defined component. Certification indicator 500 includes standard component 510 and user-defined component 520 consisting of a text string selected by the user and stored in a database with user preference information. *Id.* at 4:51–60, 7:24–25, 7:33–37. After the merchant has been authenticated, components 510 and 520 of the certification indicator are retrieved from storage and combined to form certification indicator 500, which is displayed on top of merchant's web page 100 offering computers for sale. *Id.* at 4:67–5:7.

Arent also describes computer program instructions "for performing authentication tests on web site proprietors and on other on-line transaction parties, and for authenticating data related to on-line transactions." *Id.* at 5:63–67. "The instructions also have the ability to determine whether or

not an offer presented to a user (e.g., via a web site) has been digitally signed by the party making the offer, as well as whether or not other information displayed to the user . . . is authentic." *Id.* at 6:2–6.

6. Petitioner's Proposed Combination

Petitioner asserts the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art every limitation of claims 1–32 and one of ordinary skill in the art would have reason to combine the references in the manner Petitioner proposes. Pet. 22–71. Patent Owner opposes. PO Resp. 41–79. For the reasons discussed below, we determine Petitioner has demonstrated by a preponderance of the evidence that the claims are unpatentable.

Similar to the disclosure of the '191 patent of using digital signatures to verify the authenticity of a web page, Petitioner generally relies on the description of the SHTTP document of digitally signing, by a server or third party, a document "by attaching" a digital signature to create a signed document, the authenticity of which can be verified using the digital signature. *See, e.g.*, Pet. 20 (citing Ex. 1009, 32–33); *id.* at 65 (citing Ex. 1009, 5). Petitioner further relies on the SHTTP document's disclosure of displaying a visual indicator of web page authenticity. *Id.* (citing Ex. 1009, 31) ("While preparing a secure message, the browser should provide a visual indication of the security of the transaction."). Petitioner relies on Arent's "implementation of a personalized visual indicator of authenticity" and using a visual indicator "in response to verifying the digital signature inserted into a web page." Pet. 21.

For example, regarding independent claim 1, Petitioner asserts that the SHTTP document would have conveyed to one of ordinary skill in the art "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data; and returning, from the authentication host computer, the formatted data." *Id.* at 23, 25–27. According to Petitioner, the SHTTP document's description of a server or third party digitally signing a document to create a signed document discloses the recited "transforming" (digitally signing), the recited "an authentication host computer" (a server or third party that signs the document), the recited "received data" (the document that is signed), the recited "authenticity key" (digital signature), and the recited "formatted data" (the signed document). *Id.* at 23. Also, according to Petitioner, the SHTTP document's description of placing the signed document in the cache of the server or sending it to a client discloses the recited "returning, from the authentication host computer, the formatted data." *Id.*

Petitioner asserts the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art "returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file, wherein an authenticity stamp is retrieved from the preferences file," as recited in claim 1. *Id.* at 24. According to Petitioner, showing a visual indicator of security discloses the recited "authenticity stamp." *Id.* Furthermore, Petitioner contends Arent's description of storing customization information for the visual indicator "in individual databases

for each user" discloses the recited "preferences file" from which the authenticity stamp is retrieved. *Id.*

In another example, Petitioner relies on the SHTTP document's disclosure of recursive encapsulation, a server receiving a "static pre-signed" message from a third party, and a digital signature "certificate chain" as disclosing inserting a second authenticity key, as recited in claims 10, 13, 23, and 26. *Id.*at 36 (indicating the SHTTP document discloses a second digital signature being added to a message).

7. Analysis of Patent Owner's Contentions

Patent Owner contends that Petitioner's proposed combination of the SHTTP document and Arent does not teach all of the limitations received by claims 1–32. PO Resp. 41–70. Patent Owner also contends that Petitioner fails to provide a sufficient reason to combine the teachings of the SHTTP document and Arent. PO Resp. 70–79.

In general, Patent Owner's arguments unduly focus on individual elements, without considering what the teachings of the SHTTP document—such as teachings concerning digital signatures and digitally signing documents—and Arent would have suggested to one of ordinary skill in the art regarding the claimed subject matter as a whole. *See, e.g.,* PO Resp. 46 (arguing Petitioner failed to show that SHTTP teaches "inserting"); 48 (arguing Petitioner failed to show that SHTTP teaches "returning"). In addition, Patent Owner's contentions attack an individual reference or disclosure, without consideration as to what the combined teachings would have conveyed to one of ordinary skill in the art. *See, e.g.,* PO Resp. 53–54

(contending the SHTTP document only teaches display of an unverified document).

We find these approaches to be unpersuasive in demonstrating that Petitioner has failed to meet its burden. Some of Patent Owner's contentions seem more appropriate to challenges based on anticipation, which requires a prior art reference to disclose, expressly or inherently, every limitation of the claim as arranged in the claim. *See Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). In contrast "[t]he test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art." *In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) ("[T]he test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art." (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981))). Additionally, we note the rather high level of ordinary skill in the art, which requires a bachelor's degree in computer science and at least two years of work experience, which weighs in favor of a finding of obviousness. *Innovention Toys*, 637 F.3d at 1323 ("A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse."). We also find unpersuasive contentions based on overly narrow interpretation of the claims.

We address Patent Owner's contentions *ad seriatim*.

"Transforming, at a host computer, received data"

Patent Owner contends that Petitioner's combination of the SHTTP document and Arent does not teach "transforming, at an authentication host

computer, received data," recited by independent claim 1 or similar limitations recited in claims 31 and 32. PO Resp. 42–44. According to Patent Owner, the proposed combination falls short because the claims require the authentication host computer to receive data from outside itself from another device, which the combination does not do. *Id.* Rather, Patent Owner contends, with support from its declarant, the SHTTP document only describes that the same server creates and signs a document. *Id.* at 43–44 (citing Ex. 2006 ¶¶ 22–23).

For the reasons discussed previously, we do not agree with Patent Owner that claim 1 requires the authentication host computer to receive data from outside of itself from another device. Although Patent Owner and its declarant are correct in asserting the SHTTP document describes that the same server creates and signs a document, Patent Owner's contention is insufficient in view of the scope of the challenged claims. Thus, we are not persuaded by Patent Owner's contentions that are based on incorrect interpretation of the claims.

Patent Owner does not contest that the SHTTP document discloses expressly that "a server might wish to sign the document" and applying a digital signature by attaching an appropriate certificate to the message. Ex. 1009, 5 (§ 1.4.1), 32 (§ 7.1.1). Based on this disclosure, we determine that a preponderance of the evidence weighs in favor of supporting Petitioner's contention that signing a document, as disclosed in SHTTP document, would have conveyed to one of ordinary skill in the art the recited "transforms, at an authentication host computer, received data." Pet. 23, 25.

In addition, and in response to Patent Owner's contention that signing a document is insufficient to disclose the recited "received data," Petitioner further explains, with support of its declarant, that SHTTP document discloses a software application signature process ("S-HTTP") on the server (corresponding to the recited "authentication host computer") receives data from a separate software application web process ("HTTP") on the same hardware server. Reply 4[9] (citing Ex. 1016, 13:18–14:14, 15:4–10, 25:14–26:3); *see, e.g.*, Ex. 1016, 25:4–6 (citing Ex. 1009 (SHTTP document), 8–9 (§ 2.3.3)). We agree that the SHTTP document discloses an authentication host computer receiving data from another component on the server (Reply 4 (citing Ex. 1016, 13:18–14:14, 15:4–10, 25:14–26:3)), which is not precluded by the claims and comports with the embodiment of the '191 patent that combines the authentication server logic with web server logic (Ex. 1001, 4:57–58).

[9] We note that Patent Owner had adequate notice of Petitioner's further explanation of signing digitally documents as disclosed by SHTTP document. Petitioner's position noted above was discussed in the deposition of Petitioner's declarant in response to Patent Owner's challenge that SHTTP document description of signing digitally was insufficient. *See* Ex. 1016, 13:18–14:14, 15:4–10, 25:14–26:3. Notably, Patent Owner's deposition of Petitioner's declarant took place nearly a month prior to the date when Patent Owner's Response was filed. *See* Ex. 1016 (transcript of November 25, 2014 deposition of Petitioner's declarant); Paper 21 (Patent Owner Response) filed December 22, 2014.

Inserting an Authenticity Key

Independent claims 1, 17, 31 and 32 each recite "inserting an authenticity key." Independent claims 1, 31, and 32 require inserting an authenticity key *to create* formatted (or received) data, whereas independent claim 17 recites "inserting an authenticity key *into* formatted data." Independent claim 29 does not require an authenticity key be inserted, only that formatted data has an authenticity key.

The '191 patent indicates an authenticity key can be a digital signature (*id.* at 4:14–16) and depicts an exemplary authenticity key in Figure 11 (*id.* at 2:35, 8:3–4). *See* Ex. 1002 ¶ 34 (Petitioner's declarant confirming the same). Figure 11 is set forth below:

<OBJECT ID="Checker" CLASSID="CLSID:B2157787-7492-11D4-8296-00609430A416"
CODEBASE="APge.dll"
SIGN="Tud9LuaH9v5QMQcHGUAmtDNhvZ3nGtUEHUMiGlsORV8v7JF9fp
lBiq3Jod0SvdCqQxq+4DzXc
SDK+5r6dbpJMTKiZQWLJpwNJuJSS+cfywEXdQHxcOpRt8Hryi833Bg41s
AlT+SCg5j7DBlzsvlVwohe
chGYv5476AOavkoJrD4="></OBJECT>

Figure 11 shows a few lines of various numbers and letters and, according to Petitioner's declarant, shows a digital signature. *Id.* at ¶ 34.

As noted previously, Petitioner generally relies on the description of the SHTTP document a server or third party digitally signing a document. Pet. 23, 25. Further Petitioner's declarant testifies that the SHTTP document's description of attaching a digital signature discloses the recited "inserting an authenticity key." Ex. 1002 ¶ 48. Thus, Petitioner asserts, with support from its declarant, that "transforming . . . received data by

inserting an authenticity key to create formatted data" would have been obvious in light of the disclosure of the SHTTP document of signing documents and attaching a digital signature to a message. *See, e.g.*, Pet. 23, 25.

Patent Owner contends that the broadest reasonable construction of "inserting" does not encompass "attaching" and, thus, the Petition falls short. PO Resp. 13–14, 45–47 (citing Ex. 2006 ¶ 24).[10] Petitioner opposes. Reply 2, 4–5.

In the portion of its declarant's testimony cited by Patent Owner, however, Dr. Katz does not testify that the SHTTP document does not teach "inserting an authenticity key" because the SHTTP document only discloses "attaching." Ex. 2006 ¶ 24. Rather, Dr. Katz testifies that the combination of the SHTTP document and Arent does not teach the transforming limitation because, according to Dr. Katz, the SHTTP document only

[10] We note that the parties refer to our treatment of "inserting" in our Institution Decision. PO Resp. 13–14; Reply 2. In that decision, we addressed Patent Owner's argument in its Preliminary Response argument that "inserting" did not encompass "attaching." Paper 7, 38. We determined expressly "on this [institution] record and for purposes of institution, the broadest reasonable construction of 'inserting an authenticity key' and 'insert an authenticity key' encompasses attaching an authenticity key to the received data to create formatted data." Inst. Dec. 9. Patent Owner understood the preliminary nature of our discussion of "inserting" in the Institution Decision. *See* PO Resp. 45 (noting "[the Board, based upon an initial preliminary construction," made a determination for institution purposes).

teaches "the document that is signed is a static document originating at a server or third party." *Id.*

We are not persuaded by Patent Owner's argument, which amounts to a challenge to the word "attach" in the SHTTP document without sufficient consideration of what the teachings of the SHTTP document—such as teachings concerning digital signatures and digitally signing documents—and Arent would have suggested to one of ordinary skill in the art regarding the claimed subject matter as a whole. *In re Mouttet*, 686 F.3d at 1332.

Examining the difference between the prior art's teaching of "attaching" a digital signature and the claimed subject matter as a whole, which recites "transforming . . . received data by inserting an authenticity key to create formatted data," we find the difference to be insignificant. First, the SHTTP document teaches "attaching," which involves, according to Patent Owner, attaching something "to other data," with the attached data "being kept separate from the other data." PO Resp. 14; Pet. 23, 25 (citing Ex. 1009, 32–33), 65 (citing Ex. 1009, 5). This is similar to inserting something into other data, as required by the claim. Second, the SHTTP document and the claimed subject matter both attach or insert, respectively, the same type of data—a digital signature—to other data. *See, e.g.*, Pet. 23 (indicating a digital signature corresponds to the recited "authenticity key"), 25; Ex. 1001, 4:14–18, 8:39–43 (stating "an exemplary authenticity key contains [an] hidden signature object[]," which may be an encoding of a digital signature, among other data. Third, attaching a digital signature to a document (as disclosed by the SHTTP document) at least changes the

document that is signed from not having an attachment to having an attachment. Thus, because the SHTTP document discloses changing the document, the SHTTP document discloses something remarkably similar to "transforming[11] . . . received data . . . to create formatted data," as required by the claimed subject matter.

No persuasive testimony exists in the record that inserting a digital signature would be beyond the level of ordinary skill in the art at the time of the invention. Rather, the evidence shows that digital signatures and signing digitally documents were well known and standard practice at the time of the invention. *See, e.g.*, Pet. 20 (citing Ex. 1002 ¶ 39); Ex. 1009, 5, 32–33; Ex. 1010, 3:35-39. We also note the lack of description in the plain language of the claims or the written description of the '191 patent to provide how to insert an authenticity key. Other than the claim language and the summary of invention that repeats verbatim the claim language, the '191 patent only discloses "the authenticity key is inserted into the web page." Ex. 1001, 8:1–3 (describing Fig.10, block 610); *see id.* at 1:55–57 (summary of invention). This further supports a determination that inserting (rather than attaching) a digital signature would not be beyond the level of ordinary skill in the art at the time of the invention. Notably, the '191 patent discloses a digital signature is a type of authenticity key. *See, e.g.*, Ex. 1001, Fig. 11.

---

[11] AMERICAN HERITAGE DICTIONARY 1901 (3d ed. 1992) (defining "transform" as "1. To change markedly the appearance or form of") (Ex. 3001).

For these reasons, we determine a preponderance of the evidence favors a finding that the SHTTP document would have conveyed to one of ordinary skill in the art "inserting a digital signature" and, thus, "inserting an authenticity key."

We agree with Petitioner and its declarant that the SHTTP document also would have conveyed to one of ordinary skill in the art inserting a digital signature through its description of recursive encapsulation of messages and digital signatures. Ex. 1009, 33 (§ 7.1.4); *see, e.g.*, Pet. 23 (asserting digitally signing discloses the required transformation limitation), 25 (citing Ex. 1009, 32–33); Reply 5 (discussing SHTTP document's description of placing a digital signature into underlying data in recursive encapsulation; citing Ex. 1009, 33); Hearing Tr. 8:12–10:9. In recursive encapsulation, a signed message, which includes a digital signature attached to a document, is "the inner content" of a new SHTTP message. *See id.* at Ex. 1009, 33–34. Thus, the message with a digital signature being encapsulated by another message would have conveyed that the digital signature (along with the original message) is inserted in the second message. This understanding is confirmed by Petitioner's declarant Dr. Clark testifies, such recursive encapsulation inserts "the digital signature into the underlying data and including the signed data 'as the inner content' of a new SHTTP message. Ex. 1017 ¶ 12 (citing Ex. 1009, 33).[12] In

[12] We note that Patent Owner had adequate notice of Petitioner's further explanation of signing digitally documents as disclosed by the SHTTP document. First, the SHTTP document discloses recursive encapsulation on

addition, Dr. Clark's testimony here also undercuts Dr. Katz's testimony (Ex. 2006 ¶ 24) that the SHTTP document only discloses "static" signing and, as such, would not have conveyed to one of ordinary skill in the art the required "inserting."

Returning the formatted data

Patent Owner asserts that the SHTTP document does not disclose "returning, from the authentication host computer, the formatted data," as recited in claim 1, and similar limitations recited in independent claims 31 and 32. PO Resp. 47–49. According to Patent Owner, the claim limitation "requires the formatted data to be sent by the authentication host computer to the same location from which it received the data," because such a construction is consistent with everyday examples of "returning" to the location from which an item, such as a gift or a purchase, originated. PO

---

the page frequently cited by Petitioner in its Petition regarding the SHTTP document's disclosure of digital signatures. *See* Ex. 1009, 33 (§ 7.1.4) (titled "Recursive Encapsulation"); *see, e.g.,* Pet. 25 (citing Ex. 1009, 32–33 for the "transforming" limitation in claim 1). Also, in responding in his deposition, to Patent Owner's question concerning how a document is signed in the SHTTP document, Dr. Clark described the extensions of the SHTTP protocol that inserted a signature with an encoded message as "inner content," using the MOSS ("MIME Object Security Services") or PKCS-7 format. Ex. 1015, 26:12–28:4. Notably, Patent Owner's deposition of Petitioner's declarant took place nearly a month prior to the date when Patent Owner's Response was filed. *See* Ex. 1016 (transcript of November 25, 2014 deposition of Petitioner's declarant); Paper 21 (Patent Owner Response) filed December 22, 2014. In addition, Petitioner argued this in its case in chief at the oral hearing. *See* Hearing Tr. 8:12–10:9.

Resp. 47–48. Patent Owner's declarant Dr. Katz testifies that, because claim 1 requires an authentication host computer to receive data, one of ordinary skill in the art would have understood the "returning" limitation "to require the formatted data to be returned to the same location from which the authentication host computer received the data." Ex. 2006 ¶ 25; *see* PO Resp. 48 (Ex. 2006 ¶ 25).

Petitioner opposes Patent Owner's construction but asserts that, even so, the SHTTP document teaches this limitation as interpreted by Patent Owner. Reply 5–6. According to Petitioner, the SHTTP document, in teaching the signed document is placed into the cache of the server or sent to a client when a client makes a new request to the server, would have conveyed to one of ordinary skill in the art the "returning" limitation. *See* Pet. 26 (citing Ex. 1009, 32–33). Petitioner's declarant confirms Petitioner's position. *See* Ex. 1002 ¶ 48 (citing Ex. 1009, 32–33).

Dr. Katz does not address specifically Petitioner's assertion that "placing the signed document in the cache of a server" discloses the "returning" limitation. We weigh Dr. Katz's testimony accordingly. *See, e.g.*, *Yorkey v. Diab*, 601 F.3d 1279, 1284 (holding the Board has discretion to give more weight to one item of evidence over another "unless no reasonable trier of fact could have done so"); *In re Am. Acad.*, 367 F.3d at 1368 ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations.").

We are not persuaded by Patent Owner's argument, which unduly focuses on the word "returning" in the SHTTP document without sufficient consideration of what the teachings of the SHTTP document—such as storing the signed document in its cache before sending to a client in response to a client's new request—and Arent would have suggested to one of ordinary skill in the art regarding the claimed subject matter as a whole. *In re Mouttet*, 686 F.3d at 1332.

Even assuming that the claimed "returning" requires "returning to the same location from which the data was received, after examining the differences between the prior art's teaching and the claimed subject matter as a whole, we determine the differences to be minimal. There is no persuasive evidence in the record that sending to the same location would have been beyond the skill level of one of ordinary skill in the art at the time of the invention, for instance, in view of the disclosure of sending signed documents to a client. Thus, on balance, we determine that the weight of the evidence supports Petitioner's contention, confirmed by its declarant, that the SHTTP document would have conveyed, to one of ordinary skill in the art, sending the signed document to the same location from which it was received.

Claims 31 and 32 do not require returning the formatted data to the same location from which it was received, in contrast to Patent Owner's contends (PO Resp. 49). Claim 31 does not recite receiving data from a client but only recites "format received data" a limitation that does not specify where the received data originates. Further, claim 31 recites "to

return the formatted data to *a* client" (emphasis added), a limitation that lacks an antecedent basis referring to a client recited elsewhere in the claim.

Similarly, claim 32 recites "receiving, at a client computer, formatted data from a authentication host computer wherein the authentication host computer receives the data to create received data." Claim 32 recites that the formatted data is received at a client computer. Claim 32, however, does not recite expressly from where the authentication host computer receives its data, much less expressly requiring the authentication host computer to receive its data from the client computer that receives the formatted data, as proposed by Patent Owner. PO Resp. 49.

There is no dispute that the SHTTP document discloses sending a signed document to a client. For these reasons, we determine a preponderance of the evidence favors a finding that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art "returning, from the authentication host computer, the formatted data to enable the authenticity key to be retrieved from the formatted data and to locate a preferences file," as recited in independent claim 1; "instructions to return the formatted data to a client," as recited in independent claim 31; and "receiving, at a client computer, formatted data from a authentication host computer," as recited in independent claim 32.

To enable the authenticity key to be retrieved from the formatted data and to locate a preferences file

Patent Owner argues the proposed combination of prior art does not disclose the enabling limitation as recited in independent claim 1, or

similarly recited in independent claims 17, 29, 31, and 32, because the claims require a hidden preferences file or the authenticity key to provide the to determine the location of the preferences file. PO Resp. 49–51. Previously we explained that we do not agree with Patent Owner that the claims require the formatted data or the authenticity key be used to locate the preferences file or require that the preferences file be hidden. Thus, for the reasons previously discussed, we are not persuaded Patent Owner's contentions demonstrates that Petitioner failed to meet its burden.

Retrieving an authenticity stamp from the preferences file

Regarding independent claims 1, 17, 29, 31, and 32, Patent Owner additionally contends that Arent does not disclose "retrieving an authenticity stamp from the preferences file." PO Resp. 51–52. According to Patent Owner, because Arent's certification indicator (which Petitioner alleges corresponds to the recited "authenticity stamp") is generated dynamically from components stored separately in a software wallet (which Petitioner alleges corresponds to the recited "file"), the combination of the SHTTP document and Arent does not disclose the retrieving limitation, as purportedly required by all of the independent claims. *Id.* Patent Owner further contends that none of the individual components of Arent's certification indicator "indicate that the information such as a web page has been authenticated and is from a valid source." PO Resp. 52.

We determine that Petitioner's position is supported by a preponderance of the evidence. First, the independent claims do not limit how the authenticity stamp is stored within the preferences file and so, the

claim language itself does not preclude storing the authenticity stamp as multiple components that are retrieved and then assembled. Second, the '191 patent describes that the preferences file is read "to determine the authenticity stamp and how it is to be displayed." Ex. 1001, 4:38–41. This supports Petitioner's position that Arent's disclosure of assembling a certification indicator from multiple stored components discloses the recited authenticity stamp. *See, e.g.*, Pet. 27; Reply 6–7. Third, in his deposition, Dr. Clark supported Petitioner's position and confirmed his opinion that Arent's disclosure of assembling a certification indicator from multiple stored components discloses the recited authenticity stamp. Ex. 1016, 48:18–53:13.[13]

Additionally, Patent Owner seems to argue that Arent does not disclose an authenticity stamp as arranged in the claim, an argument more appropriate to refute an anticipation challenge. PO Resp. 51–52 (contending that Arent's certification indicator is assembled from components retrieved from a file). Patent Owner's arguments do not address persuasively what the disclosure of Arent in combination with the SHTTP document would have suggested to one of ordinary skill in the art regarding the claimed subject matter as a whole. *Mouttet*, 686 F.3d at 1332.

[13] As noted previously, this deposition of Dr. Clark occurred nearly a month before Patent Owner's Response was filed.

Conclusion regarding independent claims 1, 17, 29, 31, and 32

Accordingly, we determine that Petitioner has demonstrated by preponderance of the evidence that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the additional limitations recited in independent claims 1, 17, 29, 31, and 32.

Displaying the formatted data in response to the verification of the authenticity key

Claim 4, which depends indirectly from independent claim 1 and directly depends from claim 3, further recites "displaying the formatted data in response to the verification of the authenticity key." For this additional limitation, Petitioner relies on the SHTTP document disclosure of optionally displaying unverified documents that indicate their unverified status and Arent's disclosure of displaying a wallet only after validation of a user ID and password. Pet. 30 (citing Ex. 1009, 5; Ex. 1010, 20:5–37). As Petitioner's declarant explains, the cited portion of the SHTTP document discloses displaying content only once the content is verified; "otherwise, the system reports a failure." Ex. 1002 ¶ 59 (citing Ex. 1009, 5 in opining about claim 4).

Patent Owner contends that the SHTTP document only teaches display of an unverified document, and neither the SHTTP document nor Arent teaches "either the received data or the inserted authenticity key." PO Resp. 53–54. Patent Owner's contentions amount to attacks on the references individually without consideration of what the teachings of the

references would have suggested to one of ordinary skill in the art. *See Mouttet*, 686 F.3d at 1332.

Accordingly, we determine that the Petitioner has demonstrated by preponderance of the evidence that the limitations recited in claim 4 would have been obvious to one of ordinary skill in the art.

The authenticity stamp is displayed for a graphical image within the formatted data

Claim 6, which indirectly depends from independent claim 1 and directly depends from claim 3, further recites "the authenticity stamp is displayed for a graphical image within the formatted data." Petitioner specifically relies on Arent's disclosure of a display of the certification indicator of the authentication "as a graphic that floats above the merchant web page," as shown in Arent's Figure 6. Pet. 33.

Patent Owner challenges that the display of "a graphic floating above the merchant web page" discloses the limitation further recited in claim 6. PO Resp. 54. According to Patent Owner,[14] claim 6 requires the authenticity stamp be displayed *within the formatted data*. *Id.*

Based on the '191 patent, and as confirmed by the prosecution history of the '191 patent, we do not agree with Patent Owner's interpretation of claim 6 and, thus, are not persuaded by Patent Owner's arguments predicated on a misunderstanding of the scope of claim 6. Rather than

[14] Although Patent Owner cites Dr. Katz's declaration concerning claim 10 (PO Resp. 54 (citing Ex. 2006 ¶ 27)), the cited portion of Dr. Katz's testimony does not support Patent Owner's interpretation of claim 6.

requiring the authenticity stamp be displayed *within the formatted data* (as Patent Owner contends), claim 6 requires the authenticity stamp to be displayed *for a graphical image* and the graphical image, in turn, is within the formatted data.

Further, the applicants amended claim 6 during examination to add the phrase "within the formatted data" immediately after the phrase "graphical image." Ex. 1005, 111 (amendment in response to the Office action dated July 16, 2008). *See Microsoft Corp.*, 789 F.3d at 1298 ("The PTO should also consult the patent's prosecution history in proceedings in which the patent has been brought back to the agency for a second review.").

In accordance with the precepts of English grammar, the position of the words in a sentence is the principal means of showing their relationships, and modifiers should be placed next to the words that they modify. William Strunk, Jr. & E.B. White, *The Elements of Style* 28, 30 (4th ed. 2000); *In re Hyatt*, 708 F.2d 712, 714 (Fed. Cir. 1983) ("A claim must be read in accordance with the precepts of English grammar."); *see, e.g.*, *HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1274-75 (Fed. Cir. 2012) (citing Strunk & White for the proposition that, in interpreting claim language, modifiers should be placed next to the words that they modify). Thus, a reader may assume that the graphical image is within the formatted data and the authenticity stamp is displayed for a graphical image. Claim 5, from which claim 6 directly depends, supports this assumption, because claim 5 recites "the authenticity stamp is displayed for formatted data that is verified." Thus, in claim 5, the authenticity stamp is displayed *for*

something ("formatted data that is verified") and not *within the formatted data*.

Furthermore, the '191 patent describes "an alternative embodiment" in which a web page includes graphical images of a car and a globe, and authenticity stamps also are displayed on the web page and "embedded" in each of the graphical images." Ex. 1001, 3:16–20 (referring to Fig. 3); *id.* at 2:54–57, 64–67 (referring to Fig. 2 depicting a web page 50 having an authenticity stamp 60 (depicting a diamond with text "Joe's Seal of Approval") and graphical images 58A, 58B of a car and a globe). Figure 3 of the '191 patent depicts two authenticity stamps, one for each of the two graphical images. Notably, in Figure 3 both the authenticity stamps and graphics are depicted on the web page. Thus, this alternative embodiment is consistent with an authentication stamp being displayed for a graphical image and the graphical image being within the formatted data.

We agree with Petitioner, however, that Arent's disclosure of a certification indicator that floats above the merchant web page and displayed for the web page would have conveyed the additional subject matter recited in claim 6. Pet. 33; Reply 7. We note that Arent's merchant web page depicts a "BUY" graphic image. We also note the similarly of the examples depicted Arent's Figures 4–6, on which Petitioner relies, with the alternative embodiment in Figure 3 of the '191 patent showing an authenticity stamp "A-OKAY" displayed with a graphic image (a car or a globe) displayed on a web page. More specifically, Arent's Figures 4–6 show a certification

indicator that is proof of certification of the merchant and a "BUY" graphic image displayed on a merchant's web page.

As discussed previously, the issue here is what the combination would have conveyed to one of ordinary skill in the art, not whether the prior art discloses the claimed elements as arranged in the claim. Thus, on balance and for these reasons, we determine the preponderance of the evidence favors the Petitioner's position that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the additional limitation recited in claim 6—"the authenticity stamp is displayed for a graphical image within the formatted data."

Accordingly, we determine that the Petitioner has demonstrated by preponderance of the evidence that the limitations recited in claim 6 would have been obvious to one of ordinary skill in the art.

Inserting a second authenticity key into the formatted data; validating the formatted data based on the authenticity key; receiving formatted data from a third party

Claims 10, 13, 23, and 26 each require "inserting a second authenticity key into the formatted data." For these limitations, Petitioner relies on the SHTTP document's description of recursive encapsulation in which a second digital signature can be added to a document. Pet. 36–37 (regarding claim 10), 39–40 (regarding claim 13), 49 (regarding claim 23), 54 (regarding claim 26) (all of which cite Ex. 1009, 32–33). Claim 13 and 26 each further require "validating the formatted data based on the authenticity key." For this additional limitation, Petitioner relies on the

combination of the SHTTP document and Arent. For instance, with regard to this limitation recited in claim 13, Petitioner relies on the SHTTP document's disclosure of conveying certificates for use in verifying the signature of the signed document (Ex. 1009, 13, 33) and Arent's disclosure of testing the authenticity of a merchant's supplied proof of certification (Ex. 1010, 3:55–63, Fig. 4). With regard to the same validating limitation recited in claim 26, Petitioner relies on the SHTTP document's disclosure of using cached signed documents to authenticate data (Ex. 1009, 32–33).

As an initial matter, claims 10, 13, 23, and 26 each requires performing the step of inserting an authenticity key a second time. There is insufficient evidence that repeating the inserting step is more difficult or, even, substantially different technically, than performing the inserting step the first time. Nor is there sufficient evidence that performing the step a second time would yield a new or unexpected result than performing the inserting step the first time. *See In re Harza*, 274 F.2d 669, 671 (CCPA 1960) ("It is well settled that the mere duplication of parts has no patentable significance unless a new and unexpected result is produced.").

Patent Owner challenges the "second authenticity key" limitations recited in claims 10, 13, and 23 using the same arguments that we found unpersuasive regarding inserting authenticity key recited in the independent claims. PO Resp. 55–57, 60–61, and 63–65.

Patent Owner also contends the SHTTP document's disclosure of the server receiving and caching a signed document from a third party (in Ex. 1009, 32–33) and the SHTTP document's disclosure of recursive

encapsulation (Ex. 1009, 33–34) would not have conveyed to one of ordinary skill in the art "the authentication processor is further configured to receive the formatted data having the authenticity key and, to insert a second authenticity key into the formatted data." PO Resp. 63–65. According to Patent Owner, the SHTTP document's disclosure of a server receiving a signed document from a third party relates to a "context in which the server is untrusted and does not have a signing key" and so the server, without a signing key, could not sign the received signed document a second time. *Id.*

We do not agree. As disclosed by the SHTTP document, recursive encapsulation creates a message that includes another message having a signed document. *See* Ex. 1009, 33, §§ 7.1.3–7.1.4 (stating, after discussing the server receiving a signed document in §§ 7.1.1–7.1.2, "[i]t is also possible . . . to sign the underlying data. . . . In order to do this, one would take the signed document" and, after attaching additional headers, recursively encapsulate the message so it can be sent).

Claim 22, which depends from independent claim 17, also requires the authentication processor to be configured to receive the formatted data from a third party. For this additional limitation, Petitioner relies on the SHTTP document's disclosure discussed above of receiving a signed document from a third party. Pet. 48–49 (citing Ex. 1009, 32–33); Reply 9.

Patent Owner challenges, using similar logic to that discussed previously with respect to claim 23—that the SHTTP document's server receives a signed document but does not insert an authenticity key into the formatted data. For the reasons discussed above, we are not persuaded.

Accordingly, we determine that Petitioner has demonstrated by preponderance of the evidence that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the additional limitations recited in claims 10, 13, 22, 23, and 26.

Receiving the authenticity key from a third party

Claim 11, which depends from independent claim 1, further recites "the authenticity key is received from a third-party." According to antecedent basis, the authenticity key that is inserted into the formatted data is the same authenticity key that is received from a third-party. For this additional limitation, Petitioner relies on the SHTTP document's disclosure of the server receiving a signed document from a third party, which has been discussed previously. Pet. 37 (citing Ex. 1009, 32–33). As Petitioner notes, the received signed document includes the signature. *Id.* As such, according to Petitioner, the SHTTP document would have conveyed to one of ordinary skill in the art receiving a digital signature (which according to the Petitioner corresponds to the recited "authenticity key") from a third-party.

Patent Owner contends that the SHTTP document does not disclose the additional limitation in claim 11 because the claim requires the server to receive the authenticity key and the data in which the authenticity key is to be inserted from two different devices. PO Resp. 57–58. We do not agree with Patent Owner that claim 11 precludes receiving both the data and the authenticity key from the same third party. As discussed previously, claim 1 does not specify from where the received data is received.

Furthermore, we agree with Petitioner that the SHTTP document, discloses the server receiving a document signed by a third party and, as such, discloses the received document includes an authenticity key. Ex. 1009, 32–33. Applying recursive encapsulation to the signed document (including an authenticity key) results in a new message that includes the received message, which includes the digital signature (corresponding to the recited authenticity key). Accordingly, the encapsulation of the received message having the digital signature (i.e., authenticity key) to create a new message, results in the new message having a digital signature. Because the digital signature is within the new message, the SHTTP document discloses "transforming, at an authentication host computer, received data by inserting an authenticity key to create formatted data" "wherein the authenticity key is received from a third-party." *See* Ex. 1009, 32–33, §§ 7.1.1–7.1.4. We note that the claim does not require "inserting the authenticity key" to be encoding the received data with the same authenticity key.

For the foregoing reasons, we determine that Petitioner has demonstrated by preponderance of the evidence that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the additional limitations recited in claim 11.

Retrieving additional data based on the received data

Claim 12, which depends from independent claim 1, additionally recites "retrieving additional data based on the received data." Claim 25, which depends from independent claim 17, similarly recites "the

authentication processor is further configured to receive additional data based the formatted data."

For the additional limitations received in claim 12 in its combination of the SHTTP document and Arent, Petitioner relies on Arent's disclosure of a hyperlink that allows a user to enter financial information to be used for a purchase. Pet. 38. Regarding the additional limitation recited in claim 25, Petitioner relies on Arent's disclosure of receiving order information based on the web page. Pet. 52.

Regarding claim 25, Patent Owner acknowledges Arent discloses the merchant server receives order information based on the web page. PO Resp. 67. Patent Owner contends, however, that Petitioner fails to explain how the order information is based on the merchant's web page. Patent Owner's contentions are unduly narrow in view of the broad claim language "based on" in claim 25. Because the information relates to a sales transaction with the merchant, we determine Arent's order information related to a merchant's web page is "based on" the merchant's web page.

For similar reasons, we agree the Arent's hyperlink allowing a user to enter financial information for a purchase would have conveyed to one of ordinary skill in the art retrieving additional data "based on" the received data. Patent Owner additionally asserts that the Petition is deficient regarding claim 12 because of its purported deficiency regarding "receiving data" from outside itself (PO Resp. 58–59), which we do not find persuasive for the reasons given previously.

For these reasons, we determine that Petitioner has demonstrated by preponderance of the evidence that the combination of the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the additional limitations recited in claims 12 and 25.

A plurality of images are only known by a client and challenge server.

Claims 14 and 27 each recite "a plurality of images are only known by a client and challenge server." For the limitation "a plurality of images are only known by a client and challenge server," Petitioner asserts that Arent's description of allowing a user to select a certification indicator out of a pool of media items discloses the plurality of images, as recited in claims 14 and 27. Pet. 41 (citing Ex. 1010, 4:55–58, 5:40–43), 55–56 (citing Ex. 1010, 5:37–43). There is no dispute that Arent discloses a pool of images known by a client and a server.

For the foregoing reasons, we determine that Petitioner has demonstrated by a preponderance of the evidence that the combination of SHTTP document and Arent would have conveyed to one of ordinary skill in the art "a plurality of images are only known by a client and challenge server" as recited in claims 14 and 27.[15]

---

[15] Patent Owner challenges claim 27 on the basis that Petitioner argued that Arent discloses the "claimed 'the plurality of images are *already known by a client and a challenge server*.'" PO Resp. 68 (emphasis in original). Petitioner acknowledged the typographical error in its Petition that stated "already known" instead of the recited "only known." Hearing Tr. 51:1–13. We find this error to be harmless in that claim 14 recites a nearly identical limitation "a plurality of images are only known by a client and challenge

Retrieving additional data based on the received data

Claim 24, which depends from independent claim 17, additionally recites "the authentication processor is further configured to receive a preferences key from a third party." For this additional limitation, Petitioner further relies on Arent's disclosure that preferences information may be stored on a network server site but accessed only after the user enters a user name and password from a local device. Pet. 51. According to Petitioner, the user name and password supplied from a user device would have conveyed to one of ordinary skill in the art receiving a preferences key from a third party. *Id.* Petitioner seems to reason that Arent's user name and password would have conveyed the recited "preferences key" because the user name and password are required to modify preference information. *Id.* Petitioner further seems to reason that, because a user operates a different device to supply the user name and password to the network server site, Arent's disclosure would have conveyed to one of ordinary skill in the art the network server site receiving a preferences key from a third party—another device.

Based on an exemplary embodiment disclosed in the '191 patent, Patent Owner contends that a preferences key must be a key, must be decrypted, and must determine the location of a preferences file. PO

---

server" and relied on substantially the same portions of Arent. *Compare* Pet. 41 (citing Ex. 1010, 4:55–58, 5:40–43) *with id.* at 55–56 (citing Ex. 1010, 5:37–43).

Resp. 22 (citing Ex. 1001 4:24–43), 66. We are not persuaded that the cited exemplary embodiment of the '191 patent, which mentions using a preferences key to determine the location of the preferences file, imposes such limitations on the recited "preferences key." We must be careful not to read a particular embodiment appearing in the written description into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d at 1184; *see also Superguide Corp. v. DirecTV Enters, Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004) ("Though understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not a part of the claim."); *In re Self*, 671 F.2d at 1348 (stating that it is well established that limitations not appearing in the claims cannot be relied upon for patentability).

Here, the claim language is broader than the embodiment in the '191 patent. In reciting "a preferences key," claim 24 does not relate the recited "preferences key" to another element of the claim by antecedent basis. Thus, claim 24 does not impose particular structural or functional limitations on the recited "a preferences key." Similarly, claim 24 does not relate the recited "a third party" to another element of the claim by antecedent basis or impose particular structural or functional limitations.

In view of the breadth of claim 24 and the disclosure of Arent of a user device sending a user name and password to network server site to modify preferences information, we determine that Petitioner has demonstrated by preponderance of the evidence that the combination of

SHTTP document and Arent would have conveyed "a preferences key received from a third party" to one of ordinary skill in the art.

Color or positioning of a graphic image within the formatted data is configurable

Claim 30, depends from independent claim 29 and additionally recites "at least one of color or positioning of a graphic image within the formatted data is configurable." There is no dispute that Arent discloses personalization based on color. Ex. 1010, 11:65 (indicating preferences for Wallet color could be set up); *see* Pet. 61–63 (citing Ex. 1010, 11:65). Petitioner asserts that, based on Arent's disclosures of personalization based on color and user customization of a certification indicator, the combination of SHTTP document and Arent would have conveyed to one of ordinary skill in the art the required configurable color or positioning of a graphic image within the formatted data.

Patent Owner asserts the combination is insufficient because Arent's certification indicator floats above the merchant web page, which is a contention with which we do not agree for the reasons given previously.

8. Additional Limitations Recited by Dependent Claims 2, 3, 5, 7–9, 15, 16, 18–21, and 28

Petitioner addresses each limitation of claims 2, 3, 5, 7–9, 15, 16, 18–21, and 28, which depend (directly or indirectly) from either independent claim 1 or independent claim 17. *See generally* Pet. 27–43, 46–56. Having reviewed the papers submitted by the parties and the evidence cited therein, we determine that Petitioner has demonstrated by a preponderance of the

evidence that the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the subject matter of claims 2, 3, 5, 7–9, 15, 16, 18–21, and 28.

9. Reason to Combine

We have determined that Petitioner has established by a preponderance of the evidence that the SHTTP document and Arent would have conveyed to one of ordinary skill in the art the limitations recited in claims 1–32. Our inquiry continues because "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

Petitioner contends, with support of its declarant, combining the SHTTP document and Arent would apply known technologies using known techniques and would not yield any unexpected or unpredictable results. *Id.* at 22 (citing Ex. 1002, 20). Petitioner further contends, also with support of its declarant, that one of ordinary skill in the art would have known readily how to implement the features of Arent's personalized indicators in the system described by the SHTTP document. *Id.* at 25 (citing Ex. 1002, 23). Petitioner, also with support of its declarant, provides a reason one of ordinary skill in the art would have combined the references—preventing unauthorized counterfeiting of the stamp. *Id.* at 22 (citing Ex. 1002, 20). Petitioner indicates that this reason is an advantage of using a

personalized certification indicator disclosed expressly by Arent. *Id.* (citing Ex. 1010, 4:42–50).

Patent Owner contends that Petitioner failed to provide the necessary reason to combine the teachings of the SHTTP document and Arent. PO Resp. 70–79. Patent Owner contends that Dr. Clark's testimony is unsupported and conclusory and, as such, should receive little or no weight. *Id*. at 76–79. Patent Owner also contends that Dr. Clark failed to provide objective evidence regarding the predictable combination of known techniques. *Id.* Additionally, Patent Owner contends that Dr. Clark fails to explain how the scope and the content of the prior art would have lead one of ordinary skill in the art to the claimed invention (*id.* at 76) and involves impermissible hindsight (*id.* at 75).

We find Petitioner has provided articulated reasoning with some rational underpinning. *See KSR*, 550 U.S. at 418 ("there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). Petitioner provides, with its declarant's support, articulated reasoning with some rational underpinning as to why one of ordinary skill in the art would have combined the references. Pet. 22 (citing Ex. 1002, 20). Notably, the reason given—preventing unauthorized counterfeiting of the personalized certification indicator—is disclosed expressly by Arent. Although the rote application of the teaching-suggestion-motivation test (or TSM test), requiring an express teaching in the prior art, is inappropriate, "[t]here is no necessary inconsistency between

the idea underlying the TSM test and the *Graham* analysis." *KSR*, 550 U.S. at 419.

Moreover, as noted by the Court in *KSR*, "the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416. There is no evidence that features of Arent's personalized indicators in the system described by the SHTTP document would beyond the level of one of ordinary skill in the art. The claims here are directed to computers and computer programming, not chemical processes or compounds. We again note the rather high level of ordinary skill in the art, which requires a bachelor's degree in computer science and at least two years of work experience, as another factor favoring a finding of obviousness. *Innovention Toys*, 637 F.3d at 1323 ("A less sophisticated level of skill generally favors a determination of nonobviousness . . . while a higher level of skill favors the reverse.").

Finally, Patent Owner's contentions seem to suggest bodily incorporation from one disclosed system to another is required. *Id.* at 75 (Patent Owner contends that Petitioner "failed to explain how one of ordinary skill in the arts *could* have combined the teachings" of the references) (emphasis added). A determination of obviousness is based not on bodily incorporation of parts from one disclosed system into another, but what the combined teachings would have suggested to one with ordinary skill in the art. *In re Mouttet*, 686 F.3d at 1332; *In re Keller*, 642 F.2d at 425. It is not necessary that the particular structures of the references be

physically combinable, unchanged, to render obvious the claimed invention. *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983).

10. Conclusion Regarding Obviousness

We have resolved the question of obviousness based on factual determinations of (1) the scope and content of the prior art; (2) differences between the subject matter of challenged claims and the teachings of the prior art; and (3) the level of ordinary skill in the art. *Graham*, 383 U.S. at 17–18. Patent Owner did not put forth any objective evidence of nonobviousness.

For the foregoing reasons, we determine that Petitioner has established by a preponderance of the evidence that the subject matter recited in claims 1–32 of the '191 patent as a whole would have been obvious to one of ordinary skill in the art in view of the teachings of the SHTTP document and Arent. *See* 35 U.S.C. § 103(a).

D. Patent Owner's Motion to Exclude

Patent Owner seeks to exclude "Supplemental Demonstrative Information Prepared by Paul C. Clark" (Ex. 1018). Petitioner opposes, arguing that Exhibit 1018 is Dr. Clark's notes used during his deposition. We did not refer to or rely on Exhibit 1018 in this Final Written Decision. As such, we need not reach the merits as to Patent Owner's Motion to Exclude.

Accordingly, Patent Owner's Motion to Exclude certain evidence (Ex. 1018) is dismissed as moot.

III. CONCLUSION

Petitioner has proven by a preponderance of the evidence that the subject matter of claims 1–32 of the '191 patent would have been obvious to a person of ordinary skill in the art in view of the teachings of the SHTTP document and Arent.

Patent Owner's Motion to Exclude is dismissed as moot.

IV. ORDER

Accordingly, it is hereby

ORDERED that, based on a preponderance of the evidence, claims 1–32 of U.S. Patent No7,631,191 B2 are held unpatentable;

FURTHER ORDERED that Patent Owner's Motion to Exclude is dismissed; and

FURTHER ORDERED that, because this is a Final Written Decision, the 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.

CBM2014-00100
Patent 7,631,191 B2

For PETITIONER:

Lionel M. Lavenue
lionel.lavenue@finnegan.com

Shaobin Zhu
shaobin.zhu@finnegan.com

For PATENT OWNER:

Gregory Gonsalves
gonsalves@gonsalveslawfirm.com

Andre Bahou
aj.bahou@secureaxcess.com