

No. 2016-1353

IN THE
United States Court of Appeals
for the Federal Circuit

SECURE AXCESS, LLC,

Respondent-Appellant,

– v. –

U.S. BANK NATIONAL ASSOCIATION
AND U.S. BANCORP,

Petitioners-Appellees.

**On Appeal from the United States Patent and Trademark Office,
Patent Trial and Appeal Board in No. CBM2014-00100**

PETITION FOR REHEARING *EN BANC*

Terence P. Ross
Counsel of Record
Robert T. Smith
Daniel Lipton
KATTEN MUCHIN ROSENMAN LLP
2900 K Street, NW
Suite 200 – North Tower
Washington, DC 20007
Tel: 202-625-3500
Fax: 202-339-6057
Counsel for Petitioners-Appellees

CERTIFICATE OF INTEREST

Counsel for Petitioners-Appellees U.S. Bank National Association and U.S.

Bancorp certifies the following:

1. The full name of every party or amicus represented by us is:

U.S. Bank National Association and U.S. Bancorp

2. The names of the real party in interest represented by us is:

Not applicable.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by us are:

U.S. Bank National Association is a wholly owned subsidiary of U.S. Bancorp. U.S. Bancorp is a publicly-owned corporation organized under the laws of the State of Delaware and does not have any parent corporation and no publicly-held corporation owns 10% or more of its stock.

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by us in the trial court or agency or are expected to appear in this court are:

KATTEN MUCHIN ROSENMAN LLP: Terence P. Ross, Robert T. Smith, Daniel Lipton

CROWELL & MORING LLP: Pilar Stillwater

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP: Lionel M. Lavenue, Daniel C. Cooley, Shaton C. Menzie, Shaobin Zhu

Dated: March 23, 2017

/s/ Terence P. Ross
Terence P. Ross
Counsel for Petitioners-Appellees

TABLE OF CONTENTS

CERTIFICATE OF INTEREST i

TABLE OF AUTHORITIES iii

STATEMENT OF COUNSEL..... 1

INTRODUCTION..... 1

BACKGROUND..... 6

ARGUMENT 9

I. THE PANEL MAJORITY’S DECISION CONFLICTS WITH THIS COURT’S PRECEDENT AND THE AIA, WHICH REQUIRE THE BOARD TO CONSIDER THE USES OF AN INVENTION AS DESCRIBED IN THE SPECIFICATION TO DETERMINE IF A PATENT QUALIFIES FOR CBM REVIEW..... 9

 A. This Court, Consistent with the AIA’s Text, Has Previously Affirmed the Board’s Review of the Specification to Identify CBM Patents..... 9

 B. The Panel Majority’s Decision Contradicts the Text of the AIA..... 11

 C. The Panel Majority’s Concerns About Giving the CBM Program an “Unconstrained Reach” Are Unfounded 12

II. *EN BANC* REVIEW IS NEEDED TO ENSURE THAT THE CBM REVIEW PROCESS FUNCTIONS AS CONGRESS INTENDED 13

CONCLUSION 15

CERTIFICATE OF COMPLIANCE 16

ADDENDUM A

 Panel Decision and Dissent..... A

ADDENDUM B

 U.S. Patent No. 7,631,191 B

ADDENDUM C

 Ltr. from Rep. Smith, Chairman of the House Judiciary Comm., to Sens. Kyl, Schumer, Leahy and Grassley, dated Sept. 8, 2011 C

CERTIFICATE OF SERVICE D

TABLE OF AUTHORITIES

CASES:

Apple, Inc. v. Ameranth, Inc.,
842 F.3d 1229 (Fed. Cir. 2016) 1-2, 9-10

Bilski v. Kappos,
561 U.S. 593 (2010) 3, 6

Blue Calypso, LLC v. Groupon,
815 F.3d 1331 (Fed. Cir. 2016) 9

Circuit City Stores, Inc. v. Adams,
532 U.S. 105 (2001) 13

Erlenbaugh v. United States,
409 U.S. 239 (1972) 12

SightSound Tech., LLC v. Apple Inc.,
809 F.3d 1307 (Fed. Cir. 2015) 1-2, 9

State St. Bank & Trust Co. v. Signature Fin. Grp., Inc.,
149 F.3d 1368 (Fed. Cir. 1998) 6

Unwired Planet, LLC v. Google Inc.,
841 F.3d 1376 (2016)..... 4

Versata Dev. Grp. v. SAP Amer., Inc.,
793 F.3d 1306 (Fed. Cir. 2015) 4

Vizio, Inc. v. Int’l Trade Comm’n,
605 F.3d 1330 (Fed. Cir. 2010) 11

STATUTES:

Leahy-Smith America Invents Act, Pub. L. No. 112-29,
125 Stat. 284 (2011)..... 1-2, 7, 11-13

35 U.S.C. § 112..... 2-3, 11-12, 14-15

REGULATIONS:

37 C.F.R. § 42.300 7

37 C.F.R. § 42.301 7

DECISIONS OF THE PATENT TRIAL AND APPEAL BOARD:

Agilysys, Inc. v. Ameranth, Inc.,
CBM2014-15, Paper No. 20 (P.T.A.B. Mar. 26, 2014) 4, 10

Google Inc. v. HBAC Matchmaker Media Inc.,
CMB2016-97, Paper No. 16 (P.T.A.B. Feb. 27, 2017) 5

Google Inc. v. Klaustech Inc.,
CMB2016-96, Paper No. 10 (P.T.A.B. Feb. 27, 2016) 5

Twilio Inc. v. Telesign Corp.,
CBM2016-99, Paper No. 13 (P.T.A.B. Feb. 27, 2017) 5

LEGISLATIVE MATERIALS:

H.R. Rep. No. 112-98(I) (2011)..... 6, 14

Ltr. from Rep. Smith, Chairman of the House Judiciary Comm., to Sens. Kyl,
Schumer, Leahy and Grassley, dated Sept. 8, 2011, *reprinted in* 157 Cong. Rec.
S7413-02 (daily ed. Nov. 14, 2011)..... 6, 14-15

STATEMENT OF COUNSEL

Based on my professional judgment, I believe the panel decision is contrary to the following decisions of this Court: *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229 (Fed. Cir. 2016), and *SightSound Tech., LLC v. Apple Inc.*, 809 F.3d 1307 (Fed. Cir. 2015).

In addition, based on my professional judgment, I believe this appeal requires an answer to a precedent-setting question of exceptional importance:

Whether a method patent whose claims are worded to avoid reference to financial activity, but whose specification makes plain that it is a patent “used in the practice, administration, or management of a financial product or service,” qualifies for post-grant review as a covered business method (CBM) patent under Section 18 of the Leahy-Smith America Invents Act (AIA), Pub. L. No. 112-29, § 18, 125 Stat. 284, 329-31 (2011).

/s/ Terence P. Ross

Terence P. Ross

Counsel for Petitioners-Appellees

INTRODUCTION

Under this Court’s precedent, in reviewing whether a patent qualifies for post-grant review as a covered business method (CBM) patent, the Patent Trial and Appeal Board may look not only to the express words of the claim, but also to the specification, to determine whether it is 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.*” Leahy-Smith America Invents Act (AIA), Pub. L. No. 112-29, § 18(d)(1), 125 Stat. 284, 331 (2011) (emphasis added). See *Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1236 (Fed. Cir. 2016) (“During CBM review, the Board construes claims in an unexpired patent according to their broadest reasonable construction in light of the patent’s specification.”); *SightSound Tech., LLC v. Apple Inc.*, 809 F.3d 1307, 1315 (Fed. Cir. 2015) (upholding Board’s determination that patents were CBM patents after noting that the “Board looked to the specifications” to make its determination).

Such an approach makes sense. A patent’s claim need only set out the “subject matter which the inventor or a joint inventor regards as the invention,” 35 U.S.C. § 112(b), whereas the specification is where the inventor must include “a written description of the invention, and of the manner and process of making and *using* it,” *id.* § 112(a) (emphasis added).

But a divided panel of this Court upended circuit precedent and fundamental principles of patent law by holding that, when a patent’s claim language does not expressly reference a use in financial activity, the patent cannot qualify as a CBM patent, even if the written description expressly contemplates using the invention in the practice, administration, or management of a financial product or service. Slip Op. at 19 (holding that “the statutory definition of a CBM patent *requires* that the patent have a *claim* that contains, however phrased, a financial activity element”

(emphasis added)). In other words, according to the panel majority, the “written description alone cannot substitute for what may be missing in the patent ‘claims,’ and therefore does not in isolation determine CBM status.” *Id.* at 14.

Judge Lourie dissented. He acknowledged that the patent’s claim language did not incant the magic “word ‘financial,’” but noted that the specification “clearly describes how [the patent] is ‘used in the practice’ of a financial product.” Dissenting Op. at 7. Indeed, the patent’s specification made repeated reference to the use of the claimed invention, a method for authenticating webpages, by financial institutions and their customers accessing financial products and services over the internet. “To ignore that,” Judge Lourie continued, “is to close one’s eyes to the obvious.” *Id.* Judge Lourie also rightly criticized the majority for demanding that, under the AIA, a patent must express its use in the claim language when, “[a]s a matter of patent law, claims do not necessarily need to recite uses of products.” *Id.* at 5.

If allowed to stand, the decision of the divided panel would gut the post-grant-review process that Congress enacted to cull questionable business-method patents following the Supreme Court’s decision in *Bilski v. Kappos*, 561 U.S. 593 (2010). Because patent applicants are not required to recite a use in a patent’s claims language, but need only identify uses in the patent’s specification, 35 U.S.C. § 112(a), (b), very few business-method patents will include the type of express reference to use in the claims language that the panel majority required to qualify as a CBM patent. The

effect will be to increase the cost of litigation and the threat of *in terrorem* settlement demands from the holders of dubious business-method patents.

This is not the first questionable decision by a panel of this Court concerning to scope of the CBM program. In *Versata Dev. Grp. v. SAP Amer., Inc.*, 793 F.3d 1306 (Fed. Cir. 2015), another divided panel disagreed over whether this Court even has jurisdiction to review the Board's CBM determinations. *Id.* at 1336-37 (Hughes, J., dissenting). And a petition for rehearing *en banc*, with robust *amici* support, is currently pending in *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 1376 (Fed. Cir. 2016), which asks this Court to address the level of deference owed to Board determinations that a patent qualifies for CBM status and to reconsider the holding in *Versata*.

The combination of the panel majority's decision in this case and the decision in *Unwired Planet* has already prompted the Board to reconsider its methodology for qualifying CBM patents. The Board had previously accorded CBM status to business-method patents when the specification indicated that the patent would be used in financial activity, even though the claims were not limited to a financial product or service. *See, e.g., Agilysys, Inc. v. Ameranth, Inc.*, CBM2014-15, Paper No. 20, at 9-11 (P.T.A.B. Mar. 26, 2014) (accorded CBM status to a patent even though its first claim only recited a data processing system for ordering commands and functions for "information management and synchronous communications," but where the patent's specification disclosed that it would be used to generate menus for online ordering). More recently, after *Secure Access* and *Unwired Planet*, the Board has reversed course,

concluding that, unless the patent claim is “limited” or “directed primarily” to financial activity, the patent will not qualify for CBM status, even if the specification plainly contemplates use in financial products or services. *E.g., Twilio Inc. v. Telesign Corp.*, CBM2016-99, Paper No. 13, at 11 (P.T.A.B. Feb. 27, 2017) (rejecting CBM status under *Secure Access* for internet security patent, even though embodiments in specification related to use in finance-related activities, but claims did not). In other words, under the Board’s application of *Secure Access* and *Unwired Planet*, patents that have a dual use—in financial activity and non-financial activity—no longer qualify for CBM status, regardless of the pervasiveness of their use in financial products or services. The upshot is that decisions of this Court have forced the Board, inappropriately, to read the word “only” into the AIA’s otherwise general obligation that a CBM patent be “used in the practice, administration, or management of a financial product or service.”¹

This petition, and the pending petition in *Unwired Planet*, would give this Court an opportunity to resolve the internal circuit conflict created by the panel majority’s decision in this case and address outstanding issues concerning the CBM program.

¹ See also *Google Inc. v. Klaustech Inc.*, CMB2016-96, Paper No. 10 at 12-14 (P.T.A.B. Feb. 27, 2016) (rejecting CBM status under *Unwired Planet* for internet advertising patent where claims did not recite limitations of a financial nature); *Google Inc. v. HBAC Matchmaker Media Inc.*, CMB2016-97, Paper No. 16, at 22 (P.T.A.B. Feb. 27, 2017) (rejecting CBM status under *Unwired Planet* for advertising patent where specification contained multiple references to “advertiser dollars” and “advertising revenue” but claims were not limited in scope to financial activities).

Although the CBM review program is set to expire in 2020, it is critical that it operates as intended for the next three years. The transitional program was created to weed out patents that should never have been issued in the first place. Ltr. from Rep. Smith, Chairman of the House Judiciary Comm., to Sens. Kyl, Schumer, Leahy and Grassley, dated Sept. 8, 2011, *reprinted in* 157 Cong. Rec. S7413-02 (daily ed. Nov. 14, 2011) (attached as Addendum B). And, as Congress made clear when creating it, the CBM program may ultimately be extended past the 2020 expiration date, or made permanent. *Id.*

As it stands, the panel majority's holding contradicts this Court's precedent, the plain text of Section 18 of the AIA, and the very purpose for which Congress enacted that provision into law. The Court should grant the petition for rehearing *en banc*.

BACKGROUND

Congress created the CBM post-grant review program in 2011 as part of its broader reform of patent law to “correct flaws in the system that [had] become unbearable, and to accommodate changes in the economy and the litigation practices in the patent realm.” H.R. Rep. No. 112-98(I), at 38-39 (2011). The CBM program was intended to streamline challenges to business-method patents that had been erroneously issued under this Court's decision in *State Street Bank & Trust Co. v. Signature Financial Group, Inc.*, 149 F.3d 1368 (Fed. Cir. 1998), which were later determined to be too abstract and, therefore, invalid under *Bilski v. Kappos*, 561 U.S. 593 (2010). *See* Ltr. from Rep. Smith, *reprinted in* 157 Cong. Rec. S7413-02.

The CBM post-grant review program allows parties charged with patent infringement to avoid expensive litigation over “low-quality” business-method patents that should never have been issued by providing an opportunity to invalidate such patents through administrative proceedings. *See id.*; AIA § 18(a)(1)(B). The AIA achieves this through a “Transitional Program for Covered Business Method Patents.” *Id.* § 18.

Coverage under the program turns on the definition of a “covered business method patent,” which includes two critical elements: “a patent [1] that claims a method or corresponding apparatus for performing data processing or other operations [2] used in the practice, administration, or management of a financial product or service.” AIA § 18(d)(1). (The definition excludes “technological inventions,” but that exception is not relevant here.)

Patents that fall under this CBM definition are subject to post-grant review and potential invalidation by the Board. *See id.* § 18(a). The United States Patent and Trademark Office (USPTO) issued regulations under the AIA that recite, verbatim, the statutory definition of a CBM patent, 37 C.F.R. § 42.301(a), and instruct the Board to give claims their “broadest reasonable construction in light of the specification of the patent in which it appears” when conducting a post-grant CBM review, 37 C.F.R. § 42.300(b).

The patent at issue in the panel’s decision, U.S. Patent No. 7,631,191, broadly claims a computer-security method, which utilizes an authentication key that allows

users to authenticate websites—a critical component for offering financial products and services over the internet. *See* ‘191 Patent at 12:9-14:31. Indeed, the ‘191 patent was originally developed and assigned to American Express (A471-71; A624; A1052-57), so that sensitive financial information could be transmitted without concern about having such information intercepted by a “fraudster” (A88).

The written description of the ‘191 patent explains that the patent would be used by “bank[s]”, *id.* at 1:29-34, 8:24, “credit card companies,” *id.* at 11:22-29, other “financial institutions,” *id.*, and their “customer[s] and “merchant[s],” including in the “use, sale or distribution of any goods, services or information over any network having similar functionality described herein,” *id.* at 11:17-21. For these reasons, the specification made repeated reference to phrases like: “bank computer,” “merchant computer,” “payment network,” “electronic commerce system,” and “transactions for credit cards, debit cards, and other types of financial/banking cards.” *Id.* at 11:22-67.

The eventual holder of the patent, Secure Access, does not design or market any products of its own. Instead, it has brought claims for infringement against *seventy-four* financial institutions—and only such institutions. *See* Dissenting Op. at 4-5.

Notwithstanding the many references in the patent’s written description to commercial activity, including explicit references to banking and credit card activity, the panel majority held that the patent’s repeated references to financial activity in the *specification* could not establish CBM status because the patent *claims* did not contain “a financial activity element.” Slip. Op. 19; *id.* at 14. In dissent, Judge Lourie correctly

observed that commercial activity described at length in the specification clearly contemplated that the claimed authentication method would be “‘used in the practice’ of a financial product.” Dissenting Op. at 7. Indeed, the authentication of webpages is a crucial component of all financial products and services offered over the internet.

ARGUMENT

I. THE PANEL MAJORITY’S DECISION CONFLICTS WITH THIS COURT’S PRECEDENT AND THE AIA, WHICH REQUIRE THE BOARD TO CONSIDER THE USES OF AN INVENTION AS DESCRIBED IN THE SPECIFICATION TO DETERMINE IF A PATENT QUALIFIES FOR CBM REVIEW.

A. This Court, Consistent with the AIA’s Text, Has Previously Affirmed the Board’s Review of the Specification to Identify CBM Patents.

There is no dispute that the Board must examine a patent’s claims to determine whether a patent is a CBM. *E.g., Blue Calypso, LLC v. Groupon*, 815 F.3d 1331, 1336 (Fed. Cir. 2016). But the Board has, heretofore, never been prohibited from consulting the specification to determine whether a patent qualifies for CBM status, even when the claims do not reference financial products or services.

Contrary to the panel majority’s decision, this Court has repeatedly approved the Board’s use of a patent specification to determine whether a patent qualifies for CBM review. *Ameranth*, 842 F.3d at 1236 (“During CBM review, the Board construes claims in an unexpired patent according to their broadest reasonable construction in light of the patent’s specification.”); *SightSound Tech.*, 809 F.3d at 1315 (upholding Board’s determination that patents were CBM patents after noting that the “Board

looked to the specifications” to make its determination). Significantly, in *Ameranth*, the Board accorded CBM status to the patent at issue despite the fact that its first claim only recited a data processing system for ordering commands and functions for “information management and synchronous communications,” but where the patent’s specification disclosed that it would be used to generate menus for online ordering. See *Agilysys, Inc.*, CBM2014-15, at 9-10. This Court subsequently affirmed the Board’s conclusion that the patent was a CBM patent. *Ameranth*, 842 F.3d at 1238-39.

The panel majority’s decision contradicts precedent of this Circuit by holding that “the statutory definition of a CBM patent *requires* that the patent have a *claim* that contains, however phrased, a financial activity element.” Slip Op. at 19 (emphasis added). Although the panel majority acknowledged that a claim must be understood in light of the patent’s written description, it qualified this standard by holding that “the written description alone cannot substitute for what may be missing in the patent ‘claims,’ and therefore does not in isolation determine CBM status.” *Id.* at 14. The panel majority’s decision thus precludes the Board from relying on the patent’s written description to determine whether it is a CBM patent when the claims do not expressly reference a financial activity, and it also fails to give any deference to the Board’s reasonable (and correct) interpretation of the AIA.

The panel majority’s decision also runs headlong into a well-established principle of claim construction in the Federal Circuit. Statements in the claims of intended uses are not necessarily entitled to patentable weight. Rather, statements of

intended uses must comport with the “essence or a fundamental characteristic of the claimed invention.” *Vizio, Inc. v. Int’l Trade Comm’n*, 605 F.3d 1330, 1340-41 (Fed. Cir. 2010). And to determine whether a statement of intended use is consistent with the essence of the claimed invention, this Court examines the patent’s specification and prosecution history. *Id.* at 1341 (comparing statement of intended use to specification and prosecution history). Thus, the Federal Circuit regularly examines the specifications (and other relevant patent history) to construe a patent and its usage.

B. The Panel Majority’s Decision Contradicts the Text of the AIA.

In addition to creating a conflict with Circuit precedent, the panel majority’s construction of Section 18 of the AIA misconstrues critical statutory text. The AIA defines a CBM 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). The panel majority concluded that that the term “claims” modified all subsequent text, including the second clause “used in the practice, administration, or management of a financial product or service.” Slip Op. at 12-15.

As Judge Lourie observed in dissent, the panel majority’s construction grants insufficient weight to the second clause of the CBM definition, beginning with “used in the practice.” Dissenting Op. at 7. Indeed, the panel majority’s decision to collapse the two clauses of the CBM definition is inconsistent with fundamental precepts of patent law. Whereas a patent *claim* need only set out the “subject matter

which the inventor or a joint inventor regards as the invention,” 35 U.S.C. § 112(b), the *specification* is where the inventor must include “a written description of the invention, and of the manner and process of making and *using* it,” *id.* § 112(a) (emphasis added). The CBM definition—by employing two clauses that start with the key terms “claims” and “used”—can and, indeed, should be read to embody these fundamental distinctions of patent law. That is because, in using these terms of art, Congress is presumed to appreciate such a basic distinction of patent law. *See Erlenbaugh v. United States*, 409 U.S. 239, 243 (1972) (holding that when Congress enacts a second statute that involves the “same subject” as the first, the two should be “construed ‘as if they were one law’”).

Thus, properly construed, the definition of a CBM patent consists of two distinct clauses: “a patent [1] that claims a method or corresponding apparatus for performing data processing or other operations [2] used in the practice, administration, or management of a financial product or service.” AIA § 18(d)(1). Consistent with fundamental precepts of patent law, the first clause of the CBM definition does not modify the second clause, because the uses of a patent are recited in the patent’s written description, not in the patent’s claims. 35 U.S.C. § 112(a), (b).

C. The Panel Majority’s Concerns About Giving the CBM Program an “Unconstrained Reach” Are Unfounded.

The panel majority defended its interpretation of the CBM definition on the ground that any other construction would permit “essentially every patent” to be “the

subject of a CBM petition,” because every patent can conceivably be used in a financial activity. Slip Op. at 14-15. But this concern is unfounded.

The AIA’s definition of a covered business method already contains limiting language. It applies only to a patent that claims “data processing” or “other operations.” AIA § 18(d)(1). Although “other operations,” standing alone, may seem unlimited in scope, principles of statutory construction dictate that “other operations”—a general term—must be construed as operations that are similar in kind to “data processing”—the more specific term in the same clause. *See Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 114-15 (2001) (“Where general words follow specific words . . . the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words.”).

Thus, the panel majority’s fear—that a lightbulb could be defined as a covered business method simply because it was used in a bank—is unfounded. *See* Slip. Op. at 21. The CBM definition, by its own terms, would not apply to a lightbulb because it is not a data processing or similar operation. In addition, the panel majority’s concern overlooks a key exception to the CBM definition, which has a safe harbor for “technological inventions,” such as lightbulbs. *See* AIA § 18(d)(1).

II. EN BANC REVIEW IS NEEDED TO ENSURE THAT THE CBM REVIEW PROCESS FUNCTIONS AS CONGRESS INTENDED.

The panel majority’s decision all but ensures that the vast majority of CBM patents will be disqualified from and, therefore, escape screening under the post-grant

review process enacted by Congress, because under existing patent law, patentees need not claim any use. 35 U.S.C. § 112(a), (b); *see also* Dissenting Op. at 5. This form-over-substance requirement will hobble a program intended to provide a “more efficient system for challenging patents that should not have issued,” and increase the cost of “unwarranted litigation.” H.R. Rep. No. 122-98(I), at 39-40. What is more, it will allow holders of dubious business-method patents to evade post-grant review simply by cancelling claims containing a reference to financial activity where a broader, independent claim does not include such a reference.

The panel majority’s decision conflicts with Congress’s clear intention that CBM patents be broadly defined. Indeed, one of the AIA’s authors, Chairman Smith, explained in a letter to the Senate that the AIA would establish “a presumption to allow most non-technological business method patents that have a commercial nexus into [the CBM] program for review.” Ltr. from Rep. Smith, *reprinted in* 157 Cong. Rec. S7413-02; *see also id.* at S7414 (“This program was designed to be construed as broadly as possible and as USPTO develops regulations to administer the program that must remain the goal.”).

More importantly, the legislative history includes evidence of the breadth of the CBM program in practice. For example, Chairman Smith noted that the post-grant review process established by the AIA was not limited to “one industry,” but instead would “appl[y] to non-technological patents that can apply to financial products or services.” *Id.* at S7413. Thus, contrary to the reasoning of the panel majority,

Congress plainly understood that a patent need not claim a use that is financial in nature; it was viewed as enough that the patent “*can* apply to financial products or services.” *Id.* (emphasis added).

In short, the panel majority’s decision incorrectly narrows the scope of the CBM review program, thereby insulating from review a vast number of business-method patents that never should have been issued in the first place—all because the patent at issue did not recite a financial use in the claims language. Nothing in the text or legislative history of the AIA justifies such a strained outcome, which represents a radical departure from distinctions between claims and uses embodied in well-settled patent law. *See* 35 U.S.C. § 112(a), (b).

CONCLUSION

For the foregoing reasons, the Court should grant the petition for rehearing *en banc*.

Dated: March 23, 2017

Respectfully submitted,

/s/ Terence P. Ross

Terence P. Ross

Counsel of Record

Robert T. Smith

Daniel Lipton

KATTEN MUCHIN ROSENMAN LLP

2900 K Street, NW

Suite 200 – North Tower

Washington, DC 20007

Tel: 202-625-3500

Counsel for Petitioners-Appellees

CERTIFICATE OF COMPLIANCE

This appeal was docketed prior to April 16, 2016. Accordingly, the 15-page limit of former Rule 35(b)(2) of the Federal Rules of Appellate Procedure, which was in effect prior to April 16, 2016, controls. I hereby certify that this petition is compliant with the page limit specified in former Rule 35(b)(1). It is proportionately spaced; uses a Roman-style, serif typeface (Garamond) of 14-point; and is 15 pages or less, exclusive of the material not counted under former Federal Circuit Rule 35(c)(2).

I further certify that this petition also complies with the word-volume limit specified in current Federal Rule of Appellate Procedure 35(b)(2)(A). It is proportionately spaced; uses a Roman-style, serif typeface (Garamond) of 14-point; and contains 3,722 words, exclusive of the material not counted under current Federal Circuit Rule 35(c)(2).

/s/ Robert T. Smith
Robert T. Smith
Counsel for Petitioners-Appellees

ADDENDUM A

**United States Court of Appeals
for the Federal Circuit**

SECURE AXCESS, LLC,
Appellant

v

**PNC BANK NATIONAL ASSOCIATION, U.S. BANK
NATIONAL ASSOCIATION, U.S. BANCORP, BANK
OF THE WEST, SANTANDER BANK, N.A., ALLY
FINANCIAL, INC., RAYMOND JAMES &
ASSOCIATES, INC., TRUSTMARK NATIONAL
BANK, NATIONWIDE BANK, CADENCE BANK,
N.A., COMMERCE BANK,**
Appellees

2016-1353

Appeal from the United States Patent and Trademark
Office, Patent Trial and Appeal Board in No. CBM2014-
00100.

Decided: February 21, 2017

ANDREW J. WRIGHT, Bruster PLLC, Southlake, TX,
argued for appellant. Also represented by ANTHONY KYLE
BRUSTER; ERIC M. ALBRITTON, Albritton Law Firm,
Longview, TX; ANDRE J. BAHOU, Secure Axcess, LLC,
Plano, TX; GREGORY J. GONSALVES, Falls Church, VA.

2 SECURE ACCESS, LLC v. PNC BANK NATIONAL ASSOCIATION

GREGORY H. LANTIER, Wilmer Cutler Pickering Hale and Dorr LLP, Washington, DC, argued for all appellees. Appellee PNC Bank National Association also represented by BRITTANY BLUEITT AMADI; WEI WANG, Palo Alto, CA.

TERENCE P. ROSS, Katten Muchin Rosenman LLP, Washington, DC, for appellees U.S. Bank National Association, U.S. Bancorp.

ANTHONY H. SON, Barnes & Thornburg LLP, Washington, DC, for appellees Bank of the West, Ally Financial, Inc., Cadence Bank, N.A. Appellee Cadence Bank, N.A. also represented by TONYA GRAY, Andrews Kurth LLP, Dallas, TX; SEAN WOODEN, Washington, DC.

SCOTT WESLEY PARKER, Parker Ibrahim & Berg LLC, Somerset, NJ, for appellee Santander Bank, N.A. Also represented by DIANE RAGOSA.

JASON STEWART JACKSON, Kutak Rock LLP, Omaha, NE, for appellee Raymond James & Associates, Inc.

ERIC C. COHEN, Brinks Gilson & Lione, Chicago, IL, for appellee Trustmark National Bank.

GARRET A. LEACH, Kirkland & Ellis LLP, Chicago, IL, for appellee Nationwide Bank.

MARC WADE VANDER TUIG, Senniger Powers LLP, St. Louis, MO, for appellee Commerce Bank.

Before LOURIE, PLAGER, and TARANTO, *Circuit Judges*.

Opinion for the court filed by *Circuit Judge* PLAGER.

Dissenting opinion filed by *Circuit Judge* LOURIE.

PLAGER, *Circuit Judge*.

SECURE AXCESS, LLC v. PNC BANK NATIONAL ASSOCIATION 3

This is a patent case—the issue turns on what is a covered business method patent. Appellant Secure Access, LLC (“Secure Access”) challenges a Final Written Decision of the Patent Trial and Appeal Board (“Board” or “PTAB”). As part of that decision, the Board reaffirmed its determination that the patent at issue, U.S. Patent No. 7,631,191 (“’191 patent”), owned by Secure Access, was a covered business method (“CBM”) patent under § 18 of the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284 (2011). The Board further held that claims 1–32, all the claims in the patent, were unpatentable under that statute on the grounds that they would have been obvious under the cited prior art.

On appeal, Secure Access challenges the Board’s determination to decide the case as a covered business method patent, as well as the Board’s obviousness determination. We agree with Secure Access on the first point and therefore do not reach the second. Recently, in *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 1376, 1379–82 (Fed. Cir. 2016), we concluded that the Board-adopted characterization of CBM scope in that case was contrary to the statute. We draw the same conclusion here, and further conclude that the patent at issue is outside the definition of a CBM patent that Congress provided by statute.

BACKGROUND

1. The Patent-at-Issue

Secure Access owns the ’191 patent, which issued from a continuation application of U.S. Patent Application No. 09/656,074. That parent application issued as U.S. Patent No. 7,203,838 (“’838 patent”). The ’191 and ’838 patents have substantially the same written descriptions.

The ’191 patent is entitled “System and Method for Authenticating a Web Page.” According to the patent, the “invention relates generally to computer security, and

more particularly, to systems and methods for authenticating a web page.” ’191 patent at 1:16–18. The claims generally support this broad understanding. Claims 1 and 17 are illustrative.

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.

Id. at 12:9–18; ’191 Certificate of Correction.

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.

’191 patent at 12:62–67; ’191 Certificate of Correction.

Similarly, the written description of the ’191 patent generally discusses computer security with a focus on authenticating a web page. However, on occasion, the written description contains references that might be considered to concern (at least facially) activities that are financial in nature, a consideration in determining CBM patent status.

For example, in discussing the invention, the written description explains that an Internet user might be misled to the wrong website without proper authentication. To illustrate the problem, the patent uses

“www.bigbank.com’ vs. ‘www.b[l]gbank.com’ (with an ‘l’ instead of an ‘i’).” ’191 patent at 1:31–33, *see also id.* at 8:22–24 (again, by way of example, using “bigbank.com”). Also, despite typically referring to Internet “users,” the patent occasionally refers to “customers,” *id.* at 1:28–29, and “consumers,” *id.* at 1:44. The written description further explains that “[t]he web server can be any site, for example a commercial web site, such as a merchant site, a government site, an educational site, etc.” *Id.* at 3:34–37.

In contrast to such brief references, the last several paragraphs of the written description provide several more detailed and possibly relevant references:

Moreover, while the exemplary embodiment will be described as an authentication system, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

’191 patent at 11:17–21.

The customer and merchant may represent individual people, entities, or business. The bank may represent other types of card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown.

Id. at 11:22–29. (There is no previous mention of “the bank” in the patent—there is only the “www.bigbank.com” reference. Similarly, the only previous mention of a “merchant” is the “merchant site” at 3:36, and the only previous mention of a “customer” is the “customers” at 1:28–29.)

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are possible. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, and the like.

Id. at 11:30–40. (There is no previous mention of “commerce” or a “commerce transaction” in the patent.)

For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet.

Id. at 11:46–49.

Any merchant computer and bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network. In an exemplary embodiment, the electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules

loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

Id. at 11:52–67.

2. Procedural History

At the initial decision-to-institute stage, the Board determined that the '191 patent was a CBM patent. After consolidating three separate CBM review proceedings with regard to the '191 patent, in each of which the patent was treated as a CBM patent, the Board issued the Final Written Decision at issue on appeal. *See PNC Bank, N.A. v. Secure Access, LLC*, CBM2014-00100; *Bank of the West v. Secure Access, LLC*, CBM2015-00009; *T. Rowe Price Inv. Servs., Inc. v. Secure Access, LLC*, CBM2015-00027.¹

In its Final Written Decision, the Board maintained (in keeping with its institution decisions) that the '191 patent was a CBM patent. On the merits, the Board held that claims 1–32 of the '191 patent were unpatentable because they would have been obvious under 35 U.S.C. § 103 in light of the cited prior art.

In applying the statutory test for determining whether a patent is a CBM patent, the Board quoted the statute, which is found in AIA § 18(d)(1) and which is repeated verbatim in the rules of the Patent and Trademark Office (“PTO”) at 37 C.F.R. § 42.301(a). Invoking the PTO’s rulemaking discussion and this court’s opinion

¹ In a separate proceeding, the Board declined to institute a fourth CBM review of the '191 patent. *PNC Bank, N.A. v. Secure Access, LLC*, CBM2015-00039, 2015 WL 4467374 (PTAB July 10, 2015).

8 SECURE ACCESS, LLC v. PNC BANK NATIONAL ASSOCIATION

in *Versata*, the Board rejected the patent owner's contention that the '191 patent was not a CBM patent.

The Board first rejected the patent owner's contention that the statutory phrase "financial product or service" included "only financial products such as credit, loans, real estate transactions, check cashing and processing, financial services and instruments, and securities and investment products." J.A. 9 (citation omitted).

The Board acknowledged the scope of the patent: "[t]he '191 patent relates to authenticating a web page and claims a particular manner of doing so." J.A. 10 (citing the '191 patent at 1:16–18, 12:9–18). However, the Board reasoned that because "[t]he '191 patent is directed to solving problems related to providing a web site to customers of financial institutions . . . 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." J.A. 10–11.

Despite recognizing our guidance in *Versata Development Group, Inc. v. SAP America, Inc.*, 793 F.3d 1306 (Fed. Cir. 2015), questioning the use of various legislators' competing statements in the legislative history of the AIA, the Board "note[d] 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." J.A. 11 (quoting 157 Cong. Rec. S1364–65 (daily ed. Mar. 8, 2011) (statement of Sen. Schumer)).

Further, while recognizing that the factor was not determinative, the Board observed that the patent owner's allegations of infringement by "approximately fifty finan-

SECURE AXCESS, LLC v. PNC BANK NATIONAL ASSOCIATION 9

cial 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.” J.A. 11.

The Board stated that the '191 patent disclosed “a need by financial institutions to ensure customers are confident that the financial institution’s web page is authentic.” J.A. 10 (citing the '191 patent at 1:28–33). The Board also stated that the patent disclosed “alternative embodiments of the invention as being used by financial institutions.” *Id.* (citing '191 patent at 8:21–23, 11:23–40, 11:52–67).

The Board then analyzed whether the '191 patent was for a “technological invention”—the exception to the CBM definition pursuant to AIA § 18(d)(1) and 37 C.F.R. § 42.301(b)—and determined that the '191 patent was not for a technological invention. The Board concluded its analysis of the issues, including the question of obviousness, and determined that all 32 claims of the '191 patent would have been obvious over the cited prior art and were therefore unpatentable.

Secure Axcess timely appeals the Board’s Final Written Decision; we have jurisdiction pursuant to 28 U.S.C. § 1295(a)(4)(A).

DISCUSSION

As we have noted, appellant raises two issues on appeal. First, “whether United States Patent No. 7,631,191 is a ‘covered business method’ patent subject to review under Section 18 of the AIA.” Appellant’s Br. at 6. Appellant states that “[t]his is a patent-specific question that involves an issue of first impression that has broad implications for other CBM cases: Should a patent’s eligibility for CBM review be determined on its claim language in light of the specification as understood at the

earliest effective filing date, or should the PTAB also consider post-grant evidence such as a patent owner’s litigation history?” *Id.*

The second issue raised by appellant relates to particular claim constructions made by the Board, which appellant alleges are unreasonable even under the ‘broadest reasonable interpretation’ standard the Board applied. According to appellant, the Board’s claim constructions fatally tainted the obviousness analysis.

1. Jurisdiction and Standard of Review

Neither party challenges this court’s authority to review on appeal a Final Written Decision of the Board, including, when challenged, whether the Board correctly determined that a particular patent was subject to Board review under the special provisions of AIA § 18 dealing with CBM patents. *See* 35 U.S.C. §§ 329, 141–44; *Versata*, 793 F.3d at 1314–23.

We review the Board’s determination regarding whether the ’191 patent is within the scope of the CBM statute under the Administrative Procedure Act (“APA”), specifically 5 U.S.C. § 706(2): “The reviewing court shall . . . hold unlawful and set aside agency action, findings, and conclusions found to be—(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law . . . [or] (C) in excess of statutory jurisdiction, authority, or limitations, or short of statutory right”²

Both appellant and appellees are of the view that the applicable standard of review in this case is whether the Board’s decision was arbitrary and capricious. That is incorrect. The issue here is not whether a particular

² *See Dickinson v. Zurko*, 527 U.S. 150 (1999) (the United States Patent and Trademark Office is an administrative agency and as such is subject to the APA).

patent falls within the properly-understood scope of the statutory definition of a CBM patent; rather, the issue here is whether the Board properly understood the scope of the statutory definition. That is a question of law. As we shall explain, we conclude that, as a matter of law, the statutory definition of a CBM patent precludes the Board's determination. Thus the Board acted "not in accordance with law," and "in excess of statutory jurisdiction, authority, [and] short of statutory right."³

2. The Statute and the Board's Understanding

As the Supreme Court forcefully reminds, "in interpreting a statute . . . courts must presume that a legislature says in a statute what it means and means what it says." *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253–54 (1992). In the statute before us, Congress did not leave the decision of what qualifies as a CBM patent to chance. The statute first states that "The Director may institute a

³ *SightSound Technologies, LLC v. Apple Inc.*, 809 F.3d 1307 (Fed. Cir. 2015), is miscited for the arbitrary or capricious standard. In *SightSound*, this court observed that there was no statutory-interpretation issue to be decided, because "the only legal questions regarding application of AIA § 18 were decided" by an earlier precedent of this court. *Id.* at 1315. All that was presented for decision was whether the particular patents came within the legal standards that themselves were no longer subject to dispute in the case. On that patent-specific law-application question, the court asked whether the Board's determination was arbitrary or capricious, and supported by substantial evidence. *Id.* at 1315–16. A question of legal interpretation, the statutory interpretation question that is dispositive here, is not reviewed under the 'arbitrary or capricious' or 'substantial evidence' portions of 5 U.S.C. § 706.

12 SECURE AXCESS, LLC v. PNC BANK NATIONAL ASSOCIATION

[CBM proceeding under § 18] only for a patent that is a covered business method patent.” AIA § 18(a)(1)(E).

Congress then defined 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

Id. § 18(d)(1).⁴

a. A Patent That Claims . . .

The statutory definition by its terms makes what a patent “claims” determinative of the threshold requirement for coming within the defined class. The first definitional question presented by this statutory provision is whether the requirement that the patent claim ‘something’ applies only to the first clause—*a method or corresponding apparatus for performing data processing or other operations*—or whether it applies to that clause and the second clause—*used in the practice, etc., of a financial product or service*. In order for a patent to qualify as a CBM patent, is it enough if the patent be one “that claims a method or corresponding apparatus,” as long as that method or apparatus is in fact “used in the practice . . . of a financial product or service,” even if that use is not recited, whether explicitly or implicitly, by the patent’s claims? Or must the patent contain at least one claim to the effect that the method or apparatus is “used in the practice . . . of a financial product or service”?

⁴ There is an exception, not relevant here, for “technological inventions.” For a discussion of the meaning of that term, at least as best it can be understood, see *Versata*, 793 F.3d at 1323, 1326–27.

To sharpen the question in a way relevant to this case, we must first ask, what is meant by the phrase “a patent that claims” something? Claims how, and in what terms? Must that ‘something’ be found in that part of the patent document that is toward the end of the document and preceded typically by “I (or we) claim” or “the invention claimed is,” or the equivalent? If we look to the claim as such, what role do we assign to the written description?

Though this particular statutory phrasing—“patent that claims”—is not common,⁵ when viewed in context this language would seem to have a clear meaning, whether in the usual noun form of “claim,” or, as in this case, the verb form “claims.” It invokes one of the most familiar, settled concepts in patent law, derived directly from § 112(b). It is referring to the claims of the patent, which, as properly construed, define “the scope of the patentee’s rights.” See *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 835 (2015) (quoting *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 372 (1996)). And, as the Supreme Court instructs in such circumstances, it is therefore incorporating the established meaning of “claim.” See *Evans v. United States*, 504 U.S. 255, 259–60 (1992) (quoting *Morissette v. United States*, 342 U.S. 246, 263 (1952)).⁶

⁵ It appears on only two other occasions and is nowhere defined. See 35 U.S.C. § 291 (2016); 42 U.S.C. § 262; see also 35 U.S.C. § 156 (“patent which claims”).

⁶ “[W]here Congress borrows terms of art in which are accumulated the legal tradition and meaning of centuries of practice, it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed. In such case, absence of contrary

The matter does not end there, however. A claim in a patent does not live in isolation from the rest of the patent, as if it can be cut out of the document and read with Webster’s Dictionary at hand. Established patent doctrine requires that claims must be properly construed—that is, understood in light of the patent’s written description; that is a fundamental thesis in claim construction. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–17 (Fed. Cir. 2005) (en banc). Indeed, patent drafters can be their own lexicographers, using ordinary words in unordinary ways if the drafter, in the written description, clearly so indicates. It follows that under § 18(d)(1) the written description bears importantly on the proper construction of the claims. But the written description alone cannot substitute for what may be missing in the patent “claims,” and therefore does not in isolation determine CBM status.

Returning to our earlier question, reading the statute as applying only to the first phrase in the statutory definition would give the CBM program a virtually unconstrained reach. Under that reading, a patent would qualify if it claimed a method or corresponding apparatus for performing *any* operations that happen to be used in “the practice, administration, or management of a financial product or service.” The “practice, administration, or management of a financial product or service” phrase, as earlier noted, is not limited to the financial services industry, but reaches a wide range of sales and similar transactional activity. In fact, nearly everything that is invented can and likely will be used in someone’s sale of a good or service. If that use does not have to be part of the claim as properly construed, essentially every patent could be the subject of a CBM petition—a petition filed by

direction may be taken as satisfaction with widely accepted definitions, not as a departure from them.”

any person sued for or charged with infringement at any time during the life of the CBM program.

Congress intended that the CBM program was to be more limited in scope than that. Its restriction to “covered business method” patents, and its temporary nature (eight years), make clear that it is a program established for a defined set of patents, not for virtually every patent. Moreover, in the AIA, the same statute that established the CBM program, Congress carefully set out limits on the *inter partes* review (“IPR”) program for review of patents after issuance. Persons sued for infringement had no more than one year to petition for IPR, and were restricted to presenting only certain §§ 102 and 103 grounds of unpatentability, thus excluding grounds based on, for example, § 101 or § 112. It is not sensible to read AIA § 18(d)(1) as obliterating these important limits for review of essentially any patent, subject only to the “technological invention” exception. *See* note 3, *supra*.

It follows that bifurcating the statute so that the phrase “a patent that claims” should apply only to the first phrase, and not to the entire definition Congress provided, would be radically out of keeping with the statute and congressional intent, considered in the context of other provisions in the statute.

Finally then, how are we to understand the phrase “a patent that claims”? It is the claims, in the traditional patent law sense, properly understood in light of the written description, that identifies a CBM patent. And for the reasons set out, what a qualifying patent must “claim” requires compliance with the clauses of the statutory definition.

We turn then to the second clause.

b. ... a financial product or service

The patent owner argued to the Board that the ’191 patent was ineligible for CBM review because its inven-

tion was not directed to a financial product or service and can be used by institutions other than financial institutions. Specifically, the patent owner contended that covered financial products and services were limited to products and services such as credit, loans, real estate transactions, securities and investment products, and similar financial products and services.

The Board correctly pointed out that both the Patent Office in its rulemaking discussion, and this court in its then-recent *Versata* opinion, rejected that narrow view. (The patent owner submitted its argument before the *Versata* opinion issued.) We agree that the patent owner's position before the Board is incorrect as too limiting, particularly since the argument is essentially the same one made to and rejected by us in *Versata*.

The Board, however, as part of its broader consideration of what is a "financial product or service," concluded that "[t]he 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*." J.A. 10 (emphasis added). In *Versata*, to decide this part of the case it was enough to establish our jurisdiction to adjudge the question of the Board's authority in a CBM case, and to conclude, as the Board had, that the patent in that case was a CBM patent under the statute. It was unnecessary to go further and opine about where the boundaries of the CBM definition lay.

More recently, in *Unwired Planet*, 841 F.3d at 1379–82, we were called upon to determine if the Board in that case had misstated the meaning of the statutory definition of what is a CBM patent. The Board, in determining that the patent under review was a CBM, did not limit itself to the express language of the statutory definition of a CBM patent. The Board explained that the inquiry of whether a particular patent is a CBM patent involved

determining “whether the patent claims activities that are financial in nature, *incidental to* a financial activity, or *complementary to* a financial activity.” *Id.* at 1378 (emphases added and citation omitted).

We concluded in *Unwired Planet* that the emphasized phrases are not part of the statutory definition, and when used “as the legal standard to determine whether a patent is a CBM patent [that standard] was not in accordance with law.” *Id.* at 1382. We vacated the Board’s decision and remanded for the Board to decide, in the first instance using a correct statutory definition, whether the patent at issue is a CBM patent.

In arriving at its mistaken legal standard, the Board had cited to language used by the PTO in its comments during the process of adopting regulations regarding the AIA. See, comments of the Director upon promulgation of the regulation in 2012: “[T]he legislative history explains that the definition of covered business method patent was drafted to encompass patents ‘*claiming* activities that are financial in nature, incidental to a financial activity or complementary to a financial activity.’” Transitional Program for Covered Business Method Patents—Definitions of Covered Business Method Patent and Technological Invention, 77 Fed. Reg. 48,734, 48,735 (Aug. 14, 2012) (Final Rule) (quoting 157 Cong. Rec. S5432 (daily ed. Sept. 8, 2011) (statement of Sen. Schumer)).

Despite these comments, in its final regulation defining what is a CBM patent the PTO simply adopted the statutory definition of a CBM patent without alteration or expansion. 37 C.F.R. § 42.301(a); see also *Versata*, 793 F.3d at 1323. The Board also referred to legislative history for remarks made by Senator Schumer. In *Unwired Planet* we found that no such extra-statutory sources were persuasive when the plain words of the

statute did not support such additional interpretive phrases. *See Unwired Planet*, 841 F.3d at 1381–82.

In the case before us, the Board as part of its broader discussion of what is a “financial product or service,” concluded that “[t]he 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.*” J.A. 10 (emphasis added). Consistent with *Unwired Planet*, we hold that the emphasized phrase is not a part of the statutory definition of what is a CBM patent, and, as we did in *Unwired Planet*, we conclude that such a definition of a CBM patent is beyond the scope of the statutory standard and thus “not in accordance with law.”

Blue Calypso, LLC v. Groupon, Inc., 815 F.3d 1331 (Fed. Cir. 2016), is not to the contrary. There the phrase used by the Board was “financial in nature,” which does not involve the statutory broadening at issue in *Unwired Planet*. And the court in *Blue Calypso* agreed with the Board that “financial in nature” was an accurate overall description of the challenged claims, and therefore the patent was adjudged properly under the CBM rubric. *See Blue Calypso*, 815 F.3d at 1340.

This is not a quibble over abstract phrasing. In this case, the Board’s broadened definition of a CBM patent led it, in deciding the status of the ’191 patent, to reach out beyond the question of whether the claims, as understood in light of the written description, met the statutory definition. The Board, in addition to relying on language found in the legislative history and in the PTO’s regulatory proceedings, took into consideration the litigation history of patent owner Secure Axcess in which it sued a large number of defendants who could be described as “financial” in their business activities.

But a patent owner’s choice of litigation targets could be influenced by a number of considerations, such as the

volume of a particular target's perceived infringement; the financial condition of the target; which targets are most likely to be willing to settle rather than bear the cost of litigating; available and friendly venues; and so on. Those choices do not necessarily define a patent as a CBM patent, nor even necessarily illuminate an understanding of the invention as claimed.

To be clear: the phrasing of a qualifying claim does not require particular talismanic words. When properly construed in light of the written description, the claim need only require one of a "wide range of finance-related activities," examples of which can be found in the cases which we have held to be within the CBM provision. *See Versata*, 793 F.3d at 1312–13, 1325–26; *Blue Calypso*, 815 F.3d at 1339–40; *SightSound*, 809 F.3d at 1315–16.

In sum, if a patent that fits the term *covered business method patent*, as defined in AIA § 18(d)(1), is to be usefully distinguished from all other patents, the distinction will not lie based on non-statutory phrases like "incidental to" or "complementary to" financial activity. Such phrases can have unintended consequences. For example, it is safe to assume that most, if not virtually all, inventors of methods or products claimed in a patent have some expectation that complementary financial activity will result—stated another way, that eventually their invention will produce financial rewards for their efforts. A definition that could sweep that broadly obviously will not do. Necessarily, the statutory definition of a CBM patent requires that the patent have a claim that contains, however phrased, a financial activity element.

3. The Remedy

Having determined that the Board erred in deciding this case as a CBM under its overly-broad statutory definition, we are confronted with determining the appropriate remedy. Secure Axcess, believing that the Board misapplied the statute, asks that we vacate the Board's

determination that this is a CBM patent, and remand for the Board to decide the CBM question under the correct definition.

The Board considered claims 1 and 17, among others, reproduced above, as illustrative of the claimed subject matter. J.A. at 7–8. In the course of its decision, the Board made several claim construction determinations based on its ‘broadest reasonable construction’ standard, approved by the Supreme Court in *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2142–46 (2016). Secure Axcess objects to several of these rulings, specifically those related to the issue of whether the patent requires an authenticity key to be used to, or provide the ability to, determine the location of a preferences file, and that these claim constructions tainted the court’s obviousness determinations. However that may be, for purposes of deciding whether the claims qualify the patent as a CBM patent, we find that the Board’s constructions are reasonable in light of the Board’s standard of review.⁷

In that light, and giving the patentee the broad scope available for claiming “the practice, administration, or management of a financial product or service,” we have examined with care the relevant claims as set forth earlier. Based on the record before us, and applying the definition of a CBM patent provided by Congress in AIA § 18(d), and viewed as of the earliest effective filing date, we do not find in the ’191 patent, when the claims are properly construed in light of the written description, a single claim that could qualify this patent as a “patent that claims . . . a method or corresponding apparatus . . .

⁷ See, e.g., *In re Morris*, 127 F.3d 1048 (Fed. Cir. 1997) (holding that, in reviewing a claim construction decided under the ‘broadest reasonable interpretation’ standard, we determine whether the interpretation is within the range of reasonableness).

SECURE AXCESS, LLC v. PNC BANK NATIONAL ASSOCIATION 21

used in the practice [etc.] of a financial product or service.” Like the lightbulb example in *Unwired Planet*, just because an invention could be used by various institutions that include a financial institution, among others, does not mean a patent on the invention qualifies under the proper definition of a CBM patent.

A remand to the Board for further consideration of the question whether this patent qualifies as a CBM thus would be a wasteful act, since an affirmative finding, applying the proper statutory definition, that this patent so qualifies would be, in terms of the APA standard, arbitrary or capricious. The Board’s conclusion that this is a CBM patent is reversed. The Board’s other determinations, including claim constructions as they bear on obviousness and the obviousness determination itself, are vacated.

CONCLUSION

Reversed in part; vacated in part.

COSTS

No costs.

**United States Court of Appeals
for the Federal Circuit**

SECURE AXCCESS, LLC,
Appellant

v.

**PNC BANK NATIONAL ASSOCIATION, U.S. BANK
NATIONAL ASSOCIATION, U.S. BANCORP, BANK
OF THE WEST, SANTANDER BANK, N.A., ALLY
FINANCIAL, INC., RAYMOND JAMES &
ASSOCIATES, INC., TRUSTMARK NATIONAL
BANK, NATIONWIDE BANK, CADENCE BANK,
N.A., COMMERCE BANK,**
Appellees

2016-1353

Appeal from the United States Patent and Trademark
Office, Patent Trial and Appeal Board in No. CBM2014-
00100.

LOURIE, *Circuit Judge*, dissenting.

I respectfully dissent from the majority's conclusion that the claims of the '191 patent are not directed to a covered business method ("CBM") and hence are not subject to review under AIA § 18. *See Leahy-Smith*

America Invents Act (“AIA”), Pub. L. No. 112–29, § 18, 125 Stat. 284, 329–31 (2011).¹

The statute defines a CBM 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, except that the term does not include patents for technological inventions.” *Id.* at § 18(d)(1). The claims of the ’191 patent are surely claims to “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.” *Id.* (emphasis added).

Claim 1 recites “[a] method comprising: transforming . . . received data . . . to create formatted data” ’191 patent col. 12 ll. 9–18. Claim 17 recites “[a]n 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” *Id.* col. 12 ll. 62–67. There can be little doubt that such claims meet the “method or apparatus for performing data processing” limitation of the statute.

They also meet the “financial product or service” language of the statute. Examination of the ’191 patent makes clear that the invention is to be used in the management of a financial service. The exemplary embodiment is described, *inter alia*, as follows:

The customer and merchant may represent individual people, entities, or business. The bank may represent other types of card issuing insti-

¹ Section 18 of the AIA, pertaining to CBM review, is not codified. References to AIA § 18 herein are to the statutes at large.

tutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. . . . The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, and the like. . . . Any merchant computer and bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network. In an exemplary embodiment, the electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

Id. col. 11 ll. 22–67. Similarly, the '191 patent uses “bigbank.com” as the only exemplary URL. *Id.* col. 1 ll. 29–33, col. 8 ll. 21–23. No other applications of the invention are described in the patent.

And, if there were any doubt of the use of the invention in financial management, the identity of the companies Secure Axxess, LLC (“Secure Axxess”) has sued for infringement of the '191 patent should settle the matter.

Their litigation pattern speaks volumes about what they believe their invention is “used” for.

Secure Axcess filed complaints alleging that the following companies infringe the '191 patent by “using” the invention: PNC Bank National Association, PNC Financial Services Group, Inc., U.S. Bank National Association, U.S. Bancorp, Bank of the West, BNP Paribas, Cantander Bank, N.A., Ally Financial Inc., Ally Bank, GE Capital Retail Bank, GE Capital Bank, General Electric Capital Corporation, General Electric Company, Raymond James & Associates, Inc., Raymond James Financial, Inc., Trustmark National Bank, Trustmark Corporation, Nationwide Financial Services, Inc., Nationwide Corporation, Nationwide Mutual Insurance Company, Nationwide Bank, Cadence Bank, N.A., Commerce Bank, Commerce Bancshares, Inc., Santander Bank, N.A., Vanguard Group Inc., Vanguard Marketing Corporation, Charles Schwab Bank, Charles Schwab Corporation, Ocwen Financial Corporation, Orange Savings Bank, SSB, First Financial Bank National Association, First Financial Bankshares, Inc., Texas Capital Bank, N.A., Texas Capital Bancshares, Inc., T. Rowe Price Investment Services, Inc., T. Rowe Price Associates, Inc., T. Rowe Price Group, Inc., Bank of America Corporation, Bank of America, N.A., A.N.B. Holding Company, Ltd., American National Bank of Texas, Arvest Bank Group, Inc., Arvest Bank, Austin Bankcorp, Inc., Austin Bank, Texas N.A., Bank of the Ozarks, Inc., Bank of the Ozarks, Citizens 1st Bank, Compass Bancshares, Inc., Compass Bank, Cullen/Frost Bankers, Inc., the Frost National Bank, Diboll State Bancshares, Inc., First Bank & Trust East Texas, First Community Bancshares, Inc., First National Bank Texas, First National of Nebraska, Inc., First National Bank of Omaha, First National Bank Southwest, Sterling Bancshares, Inc., Sterling Bank, Harris Bankcorp., Inc., Harris N.A., Intouch Credit Union, Credit Union, ING Direct Bancorp, ING Bank, FSB, North Dallas Bank &

SECURE AXCESS, LLC v. PNC BANK NATIONAL ASSOCIATION 5

Trust Co., Zions Bancorportion, Zions First National Bank, and Amegy Bank N.A.

Moreover, at oral argument, Secure Axcess’s counsel, in response to a question, stated that no companies have been sued other than financial institutions. Oral Argument at 7:15–7:30, *Secure Axcess, LLC v. PNC Bank N.A.*, No. 16-1353 (Fed. Cir. Nov. 2, 2016), available at http://www.cafc.uscourts.gov/oral-argument-recordings?-title=&field_case_number_value=2016-1353&field_date_value=2016-11-02&field_date_value2=2016-11-02&field_date_value3=2016-11-02&field_date_value4=2016-11-02&field_date_value5=2016-11-02&field_date_value6=2016-11-02&field_date_value7=2016-11-02&field_date_value8=2016-11-02&field_date_value9=2016-11-02&field_date_value10=2016-11-02&field_date_value11=2016-11-02&field_date_value12=2016-11-02&field_date_value13=2016-11-02&field_date_value14=2016-11-02&field_date_value15=2016-11-02&field_date_value16=2016-11-02&field_date_value17=2016-11-02&field_date_value18=2016-11-02&field_date_value19=2016-11-02&field_date_value20=2016-11-02&field_date_value21=2016-11-02&field_date_value22=2016-11-02&field_date_value23=2016-11-02&field_date_value24=2016-11-02&field_date_value25=2016-11-02&field_date_value26=2016-11-02&field_date_value27=2016-11-02&field_date_value28=2016-11-02&field_date_value29=2016-11-02&field_date_value30=2016-11-02&field_date_value31=2016-11-02&field_date_value32=2016-11-02&field_date_value33=2016-11-02&field_date_value34=2016-11-02&field_date_value35=2016-11-02&field_date_value36=2016-11-02&field_date_value37=2016-11-02&field_date_value38=2016-11-02&field_date_value39=2016-11-02&field_date_value40=2016-11-02&field_date_value41=2016-11-02&field_date_value42=2016-11-02&field_date_value43=2016-11-02&field_date_value44=2016-11-02&field_date_value45=2016-11-02&field_date_value46=2016-11-02&field_date_value47=2016-11-02&field_date_value48=2016-11-02&field_date_value49=2016-11-02&field_date_value50=2016-11-02&field_date_value51=2016-11-02&field_date_value52=2016-11-02&field_date_value53=2016-11-02&field_date_value54=2016-11-02&field_date_value55=2016-11-02&field_date_value56=2016-11-02&field_date_value57=2016-11-02&field_date_value58=2016-11-02&field_date_value59=2016-11-02&field_date_value60=2016-11-02&field_date_value61=2016-11-02&field_date_value62=2016-11-02&field_date_value63=2016-11-02&field_date_value64=2016-11-02&field_date_value65=2016-11-02&field_date_value66=2016-11-02&field_date_value67=2016-11-02&field_date_value68=2016-11-02&field_date_value69=2016-11-02&field_date_value70=2016-11-02&field_date_value71=2016-11-02&field_date_value72=2016-11-02&field_date_value73=2016-11-02&field_date_value74=2016-11-02&field_date_value75=2016-11-02&field_date_value76=2016-11-02&field_date_value77=2016-11-02&field_date_value78=2016-11-02&field_date_value79=2016-11-02&field_date_value80=2016-11-02&field_date_value81=2016-11-02&field_date_value82=2016-11-02&field_date_value83=2016-11-02&field_date_value84=2016-11-02&field_date_value85=2016-11-02&field_date_value86=2016-11-02&field_date_value87=2016-11-02&field_date_value88=2016-11-02&field_date_value89=2016-11-02&field_date_value90=2016-11-02&field_date_value91=2016-11-02&field_date_value92=2016-11-02&field_date_value93=2016-11-02&field_date_value94=2016-11-02&field_date_value95=2016-11-02&field_date_value96=2016-11-02&field_date_value97=2016-11-02&field_date_value98=2016-11-02&field_date_value99=2016-11-02&field_date_value100=2016-11-02

It is true that the word “financial” does not appear in the claims. However, that fact should not decide this case. *See Versata Dev. Grp., Inc. v. SAP Am., Inc.*, 793 F.3d 1306, 1325 (Fed. Cir. 2015) (holding that “the definition of ‘covered business method patent’ is not limited to products and services of only the financial industry, or to patents owned by or directly affecting the activities of financial institutions”); *see also Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1338 (Fed. Cir. 2016) (affirming Board’s decision “declin[ing] to limit application of CBM review to patent claims tied to the financial sector”); *SightSound Techs., LLC v. Apple Inc.*, 809 F.3d 1307, 1315 (Fed. Cir. 2015) (explaining *Versata* “foreclosed” limiting the CBM patent definition to patents “directed to the management of money, banking, or investment or credit”). As a matter of patent law, claims do not necessarily need to recite uses of products. Certainly, claims to products or apparatuses do not (note that AIA § 18(d)(1) refers to a “method or corresponding apparatus”). And, if a method claim otherwise satisfies the requirements of 35 U.S.C. § 112, it need not recite an ultimate use.

The written description of the ’191 patent, in accordance with the requirements of the statute, *see* 35 U.S.C. § 112 (“The specification shall contain a written description of the invention, and of the manner and process of . . . using it . . .”), tells us that the invention is to be used for

financial management. *See* '191 patent col. 11 ll. 22–67; *see also id.* col. 1 ll. 29–33, col. 8 ll. 21–23. The inventors, complying with the statute, thus told us what the invention is to be used for. The claims recite an invention *used in the practice* of a financial product, and the uses are described in the written description of the patent.

In my view, the Board correctly concluded that the “method and apparatus claimed by the '191 patent perform operations used in the practice, administration, or management of a financial product or service,” in accordance with the CBM patent statutory definition. *PNC Bank, N.A. v. Secure Access, LLC*, No. CBM2014-00100, 2015 WL 5316490, at *5 (P.T.A.B. Sept. 8, 2015). It is true that the Board also used overly broad language in stating in the alternative that the “method and apparatus claimed by the '191 patent . . . *are incidental to a financial activity.*” *Id.* (emphasis added). And the Board did state 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.” *Id.* at *6. But overstatement does not change the basic fact that, as the written description of the patent itself indicates, the invention is directed to a method and apparatus used in financial management, as referred to in the statute. *See, e.g., Blue Calypso*, 815 F.3d at 1339 n.2 (explaining the Board correctly concluded that claims referring to “an incentive program” were eligible for CBM review where the patent “repeatedly, and almost exclusively discloses ‘incentive’ and ‘incentive program’ in a financial context”) (internal citation omitted).

I do recognize that the Board’s overly broad language, *i.e.*, “incidental to a financial activity,” has now been cabined by our recently issued decision in *Unwired Planet, LLC v. Google Inc.*, 841 F.3d 1376 (Fed. Cir. 2016). That curtailment should not cause this panel to topple over an otherwise sound decision by the Board in this case that the '191 patent is directed to financial management.

Such a decision was not based only on the forbidden language. *See PNC Bank*, 2015 WL 5316490, at *10 (“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.”).

The majority attempts to escape the clear purport of the invention by ranging into a discussion of the meaning of claims in patent law. Its use of language such as “on occasion,” “might be considered,” and “at least facially” pointedly overlooks the nature of the invention and the meaning of the statute. The opinion has subsections headed “A patent that claims . . .” and “. . . a financial product or service,” but it virtually ignores the statutory language “used in the practice.” The written description clearly describes how this invention is “used in the practice” of a financial product. And, while not conclusive, the post-issuance litigation history makes the point unmistakable. To ignore that is to close one’s eyes to the obvious.

The majority disparages the clear use of this invention in the practice of a financial product or service by worrying that the CBM program would have “virtually unconstrained reach” and that “a patent would qualify [for CBM review] if it claimed a method or corresponding apparatus for performing *any* operations that happen to be used in ‘the practice, administration, or management of a financial product or service.’” The answer to such concerns is that we need not probe the limits of the statutory language by reciting all sorts of non-financial products to show that a sensible interpretation of this statute must include what Secure Axxess itself considers a financial product. Common sense is not precluded from use in

8 SECURE ACCESS, LLC v. PNC BANK NATIONAL ASSOCIATION

interpreting statutes and claims. Suffice it to say that the relation of this invention to the financial world is one of substantial identity compared with an incidentally-used invention like a lightbulb or ditch-digging. *Cf. Unwired Planet*, 841 F.3d at 1382.

I therefore respectfully dissent from the conclusion that the '191 patent is not a CBM patent.

ADDENDUM B



US007631191B2

(12) **United States Patent**
Glazer et al.

(10) **Patent No.:** **US 7,631,191 B2**
(45) **Date of Patent:** ***Dec. 8, 2009**

(54) **SYSTEM AND METHOD FOR AUTHENTICATING A WEB PAGE**

(58) **Field of Classification Search** 713/201,
713/180, 176
See application file for complete search history.

(76) **Inventors:** **Elliott Glazer**, 14107 Chiasso Ter., Chesterfield, VA (US) 23838; **Dirk White**, 6638 W. Via Montoya, Glendale, AZ (US) 85310; **David Armes**, 4035 W. Banff La., Phoenix, AZ (US) 85033; **Fred Alan Bishop**, 2811 W. Dynamite Blvd., Phoenix, AZ (US) 85085; **Michael Barrett**, 9182 E. Carribean La., Scottsdale, AZ (US) 85260

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,261,043 A 11/1993 Wolber et al.
5,365,360 A 11/1994 Torres

(Continued)

FOREIGN PATENT DOCUMENTS

WO WO9750036 12/1997

OTHER PUBLICATIONS

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 182 days.

Nayem Isiam, Rangachari Anand, Trent Jaeger, and Josyula R. Rao; "A Flexible Security Model for Using Internet Content"; Jun. 28, 1997.

(Continued)

This patent is subject to a terminal disclaimer.

Primary Examiner—Kambiz Zand
Assistant Examiner—William S Powers

(74) *Attorney, Agent, or Firm*—Snell & Wilmer L.L.P.

(21) **Appl. No.:** **11/423,340**

(57) **ABSTRACT**

(22) **Filed:** **Jun. 9, 2006**

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 of the icon and is not merely a copy. The method includes a user requesting a web page from a web site using a web browser. The web server receives the request, retrieves the web page and forwards it to an authentication server. The authentication server inserts an authenticity key into the web page, then the page (including the authenticity key) is returned to the user. If the page includes an authenticity key, the authenticity is verified at the user's computer because the user computer includes logic (e.g., software) to verify the authenticity. During the user configuration process, the user defines an authenticity stamp which determines the format of an authenticated page.

(65) **Prior Publication Data**

US 2006/0218391 A1 Sep. 28, 2006

Related U.S. Application Data

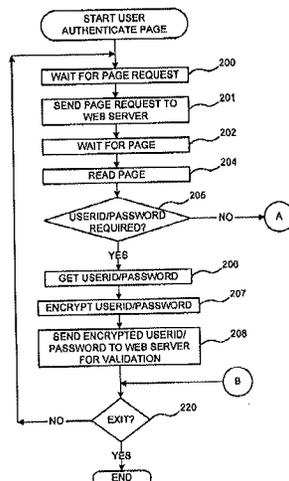
(63) Continuation of application No. 09/656,074, filed on Sep. 6, 2000, now Pat. No. 7,203,838.

(60) Provisional application No. 60/153,004, filed on Sep. 9, 1999.

(51) **Int. Cl.**
H04L 9/32 (2006.01)

(52) **U.S. Cl.** 713/176

32 Claims, 12 Drawing Sheets



US 7,631,191 B2

Page 2

U.S. PATENT DOCUMENTS

5,497,422 A 3/1996 Tysen et al.
 5,530,856 A 6/1996 Dahod et al.
 5,606,609 A * 2/1997 Houser et al. 713/179
 5,752,022 A 5/1998 Chiu et al.
 5,765,176 A 6/1998 Bloomberg
 5,809,317 A 9/1998 Kogan et al.
 5,872,850 A * 2/1999 Klein et al. 705/51
 5,889,868 A 3/1999 Moskowitz et al.
 5,890,170 A 3/1999 Sidana
 5,892,904 A 4/1999 Atkinson et al.
 5,893,127 A 4/1999 Tyan et al.
 5,905,800 A 5/1999 Moskowitz
 5,907,619 A 5/1999 Davis
 5,930,792 A 7/1999 Polcyn
 RE36,444 E 12/1999 Sanches Frank et al.
 6,016,491 A 1/2000 Kou
 6,247,047 B1 6/2001 Wolff
 6,286,001 B1 * 9/2001 Walker et al. 707/9
 6,366,912 B1 * 4/2002 Wallent et al. 707/9
 6,453,416 B1 * 9/2002 Epstein 713/170
 6,539,093 B1 3/2003 Asad et al.
 6,618,717 B1 9/2003 Karadimitriou et al.
 6,681,017 B1 * 1/2004 Matias et al. 380/277

6,735,694 B1 5/2004 Berstis et al.
 6,778,986 B1 8/2004 Stern et al.
 6,785,717 B1 8/2004 Nickerson et al.
 2001/0056487 A1 12/2001 Yoo
 2002/0002543 A1 1/2002 Spooren et al.
 2002/0029252 A1 3/2002 Segan et al.
 2002/0124172 A1 9/2002 Manahan
 2003/0023878 A1 1/2003 Rosenberg et al.
 2003/0093699 A1 5/2003 Banning et al.
 2003/0110384 A1 6/2003 Carro
 2003/0131048 A1 7/2003 Najork
 2003/0158823 A1 8/2003 Fulton et al.
 2004/0078452 A1 4/2004 Jamieson

OTHER PUBLICATIONS

Network Working Group; "The Secure HyperText Transfer Protocol"; also available on <http://www.landfield.com/rfc/rfc2660.html>.
 "Test of Signal HTML"; also available on http://www.crafeidl.ac.uk/docs/email/pgp/html/signed_html.html.
 "PGP Signed Web-Pages"; also available on <http://www.pobox.com/~ejnbell/pgp-www.html>.
<http://www-server.bcc.ac.uk/~ccaamrg/seal/seal.html> (site not accessible).

* cited by examiner

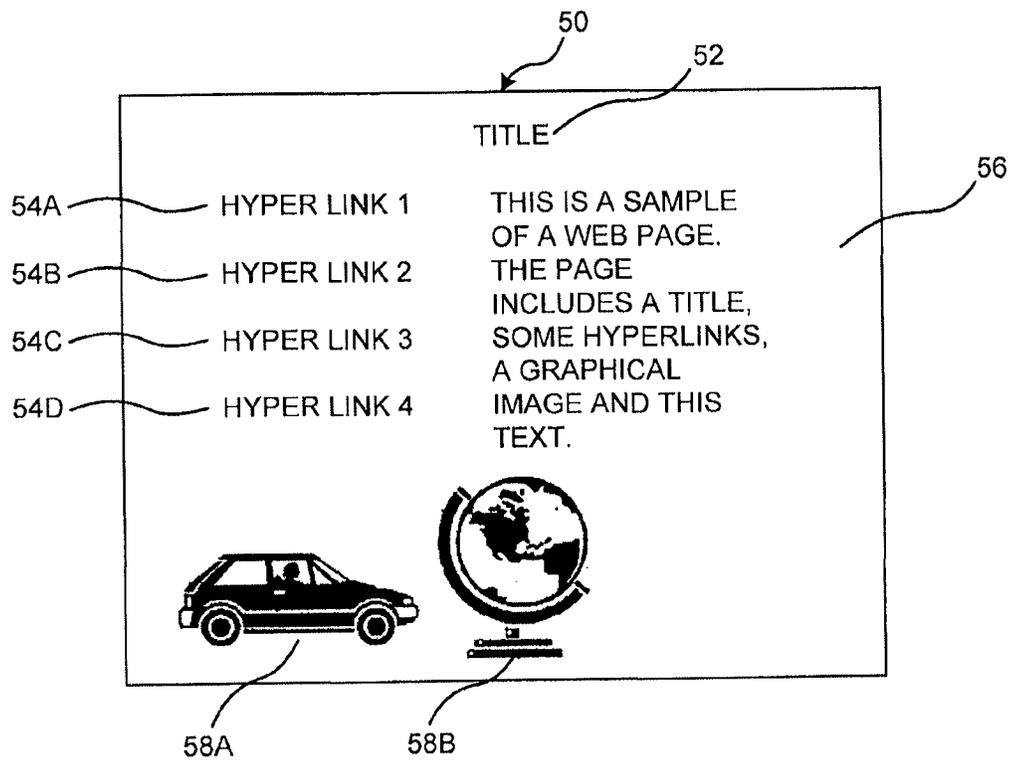


FIG. 1

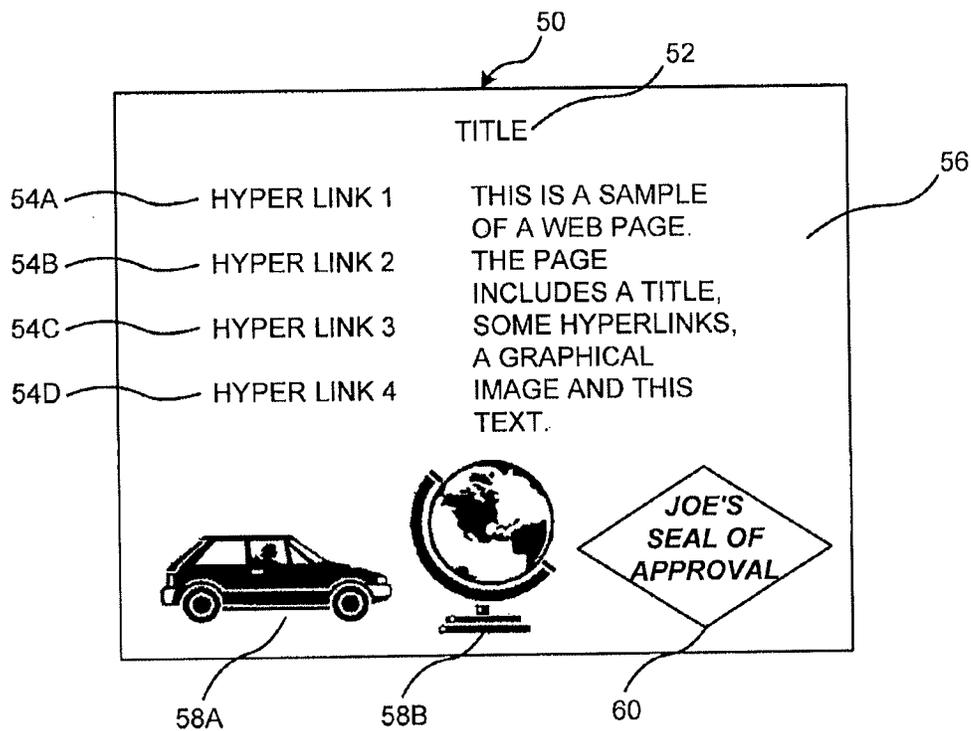


FIG. 2

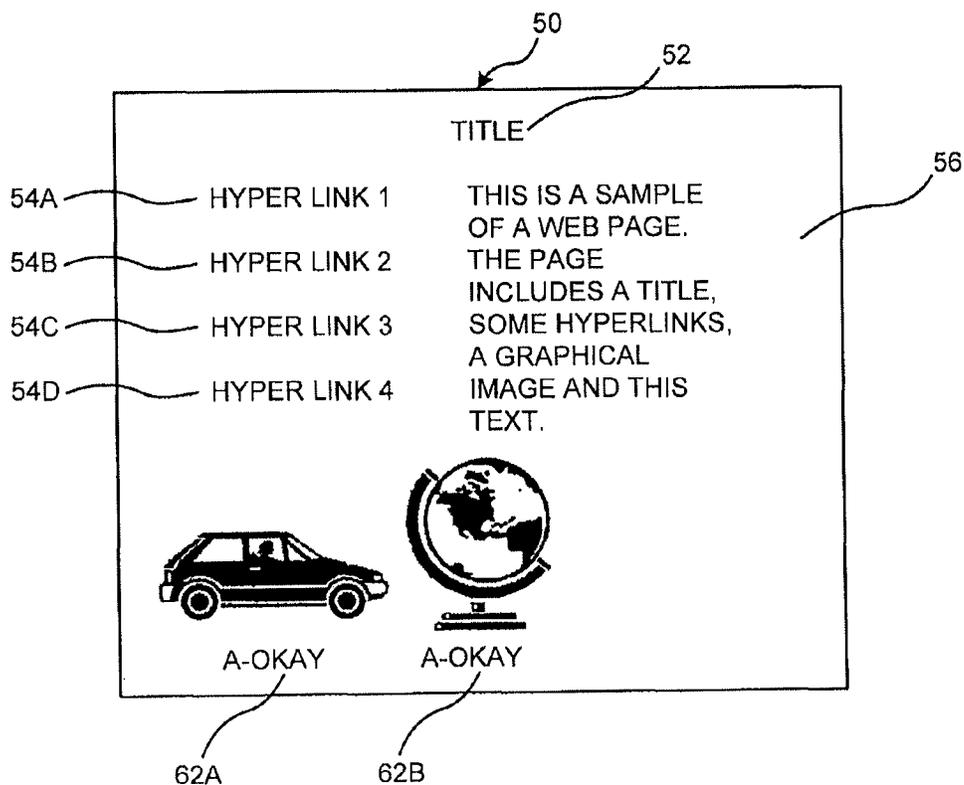


FIG. 3

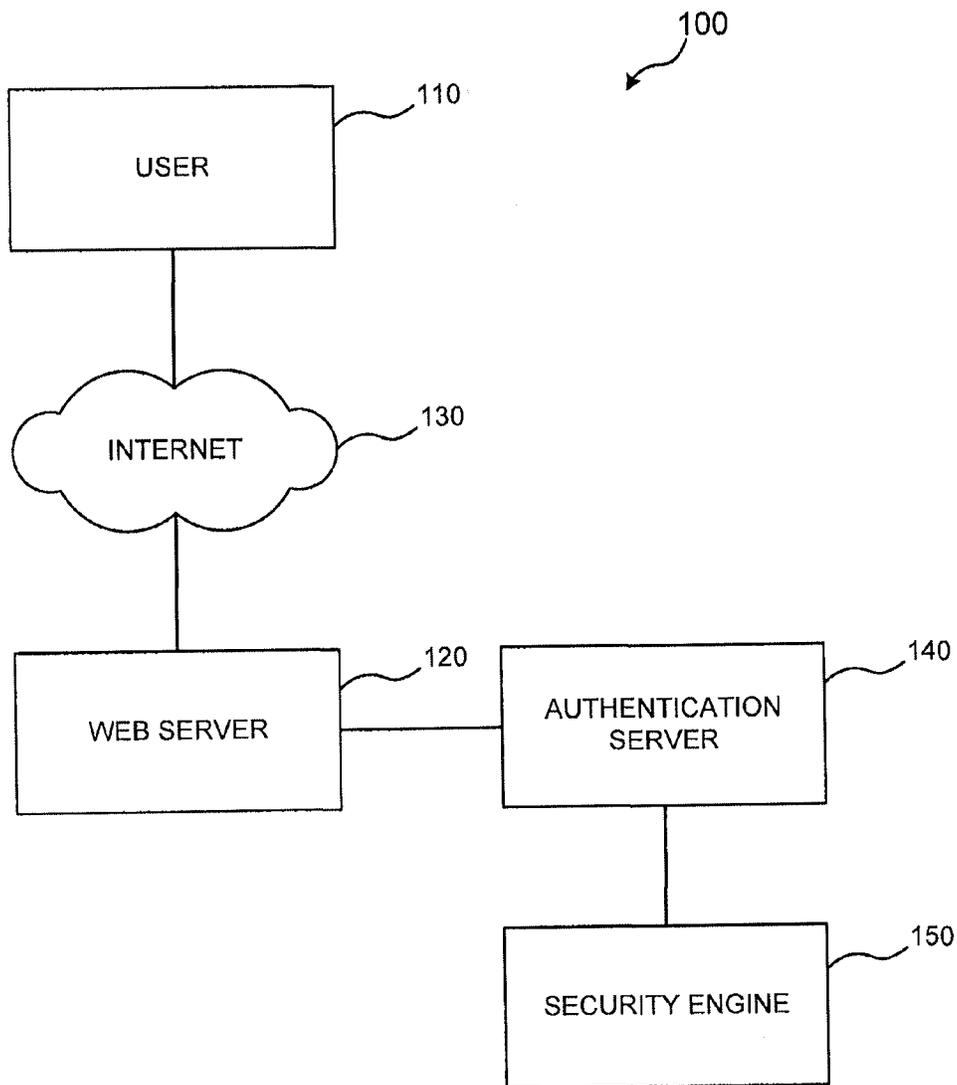


FIG. 4

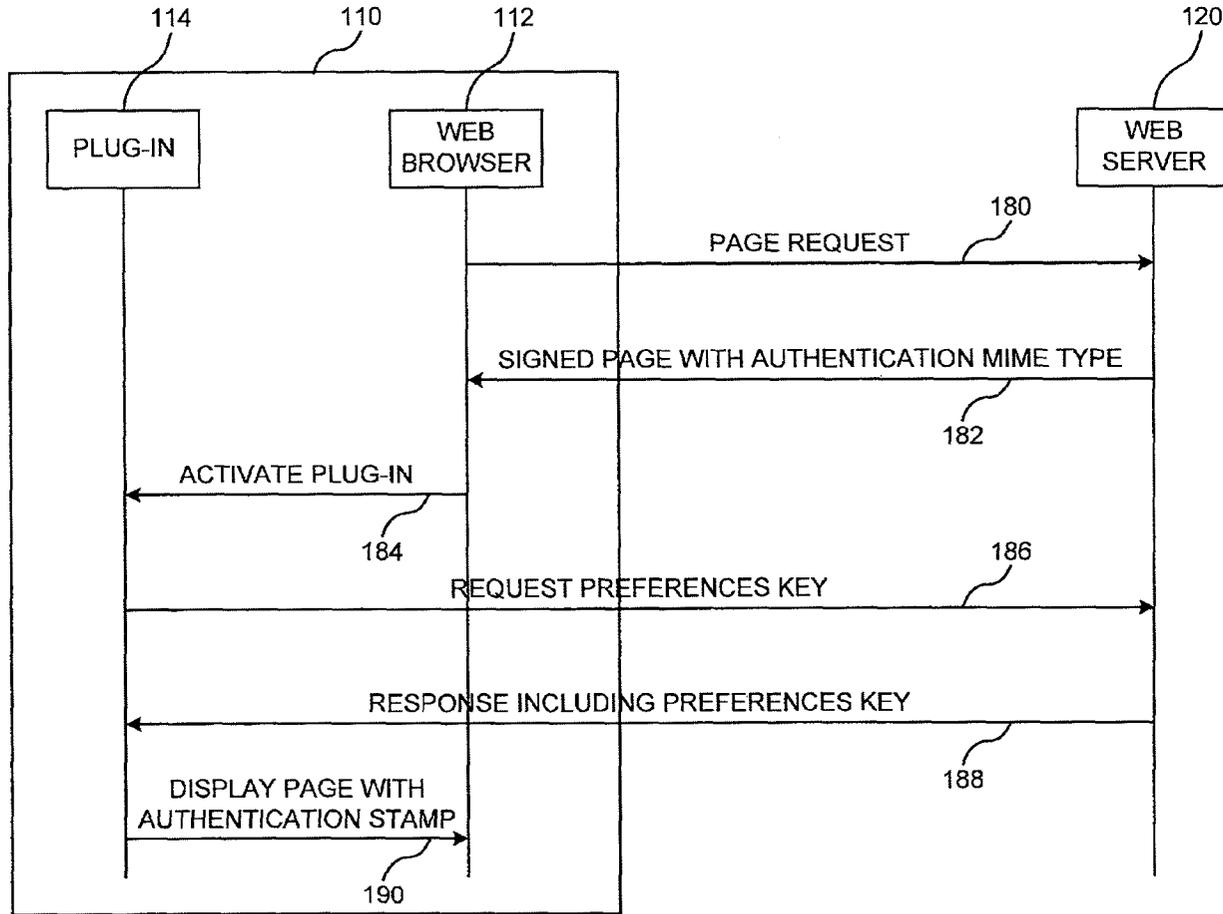


FIG. 5

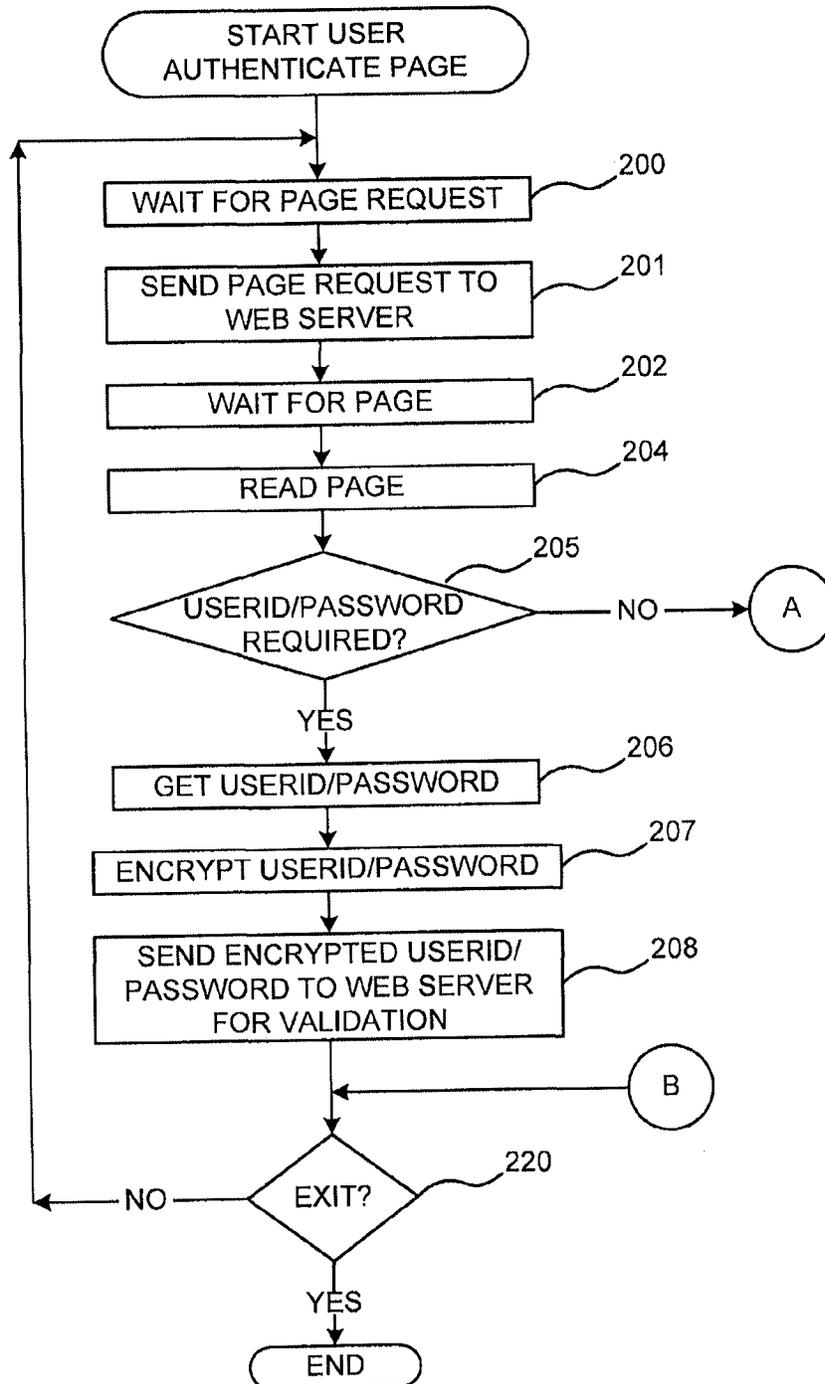


FIG. 6A

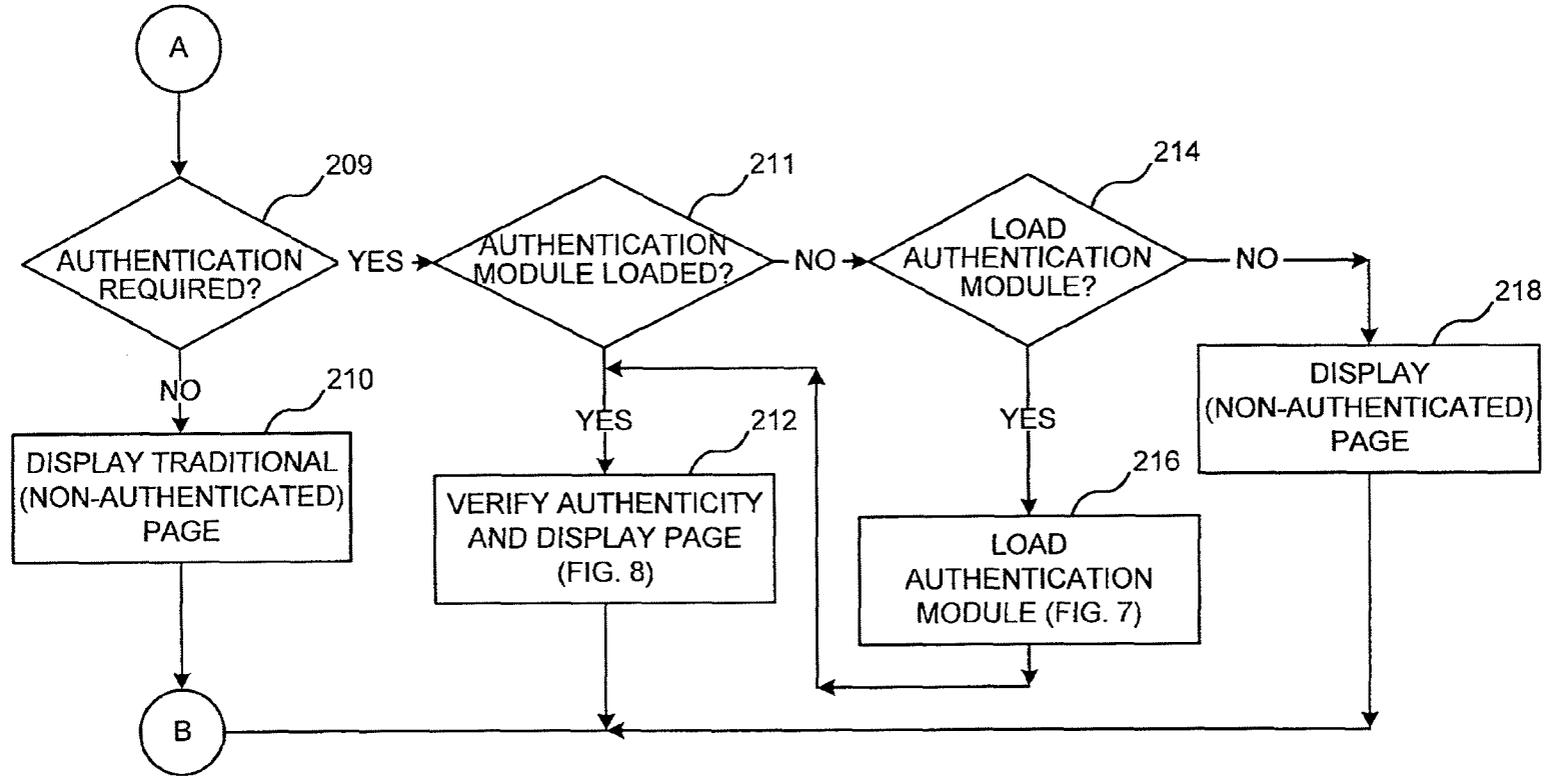


FIG. 6B

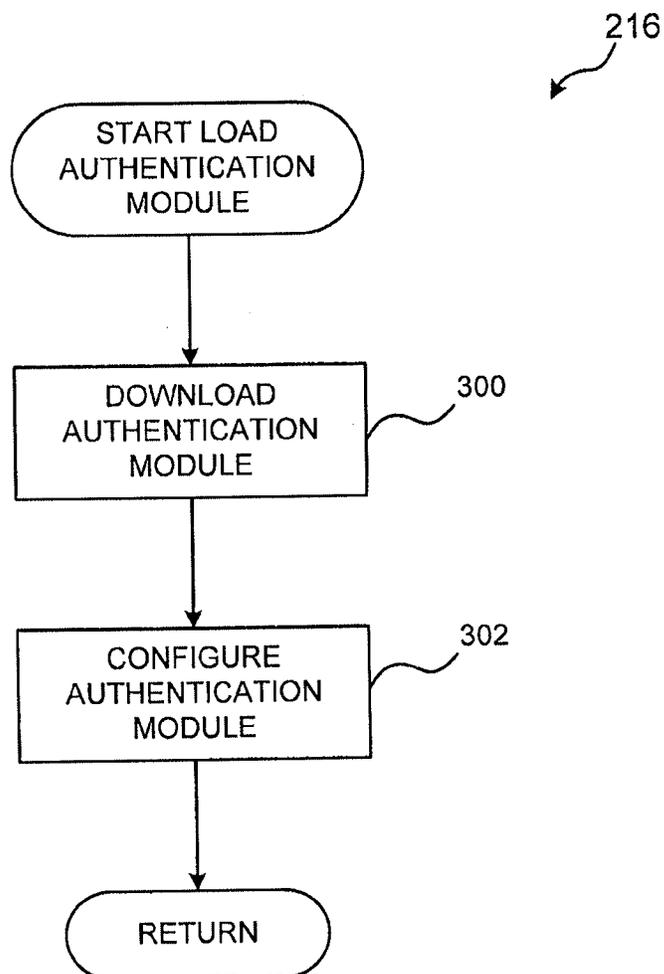


FIG. 7

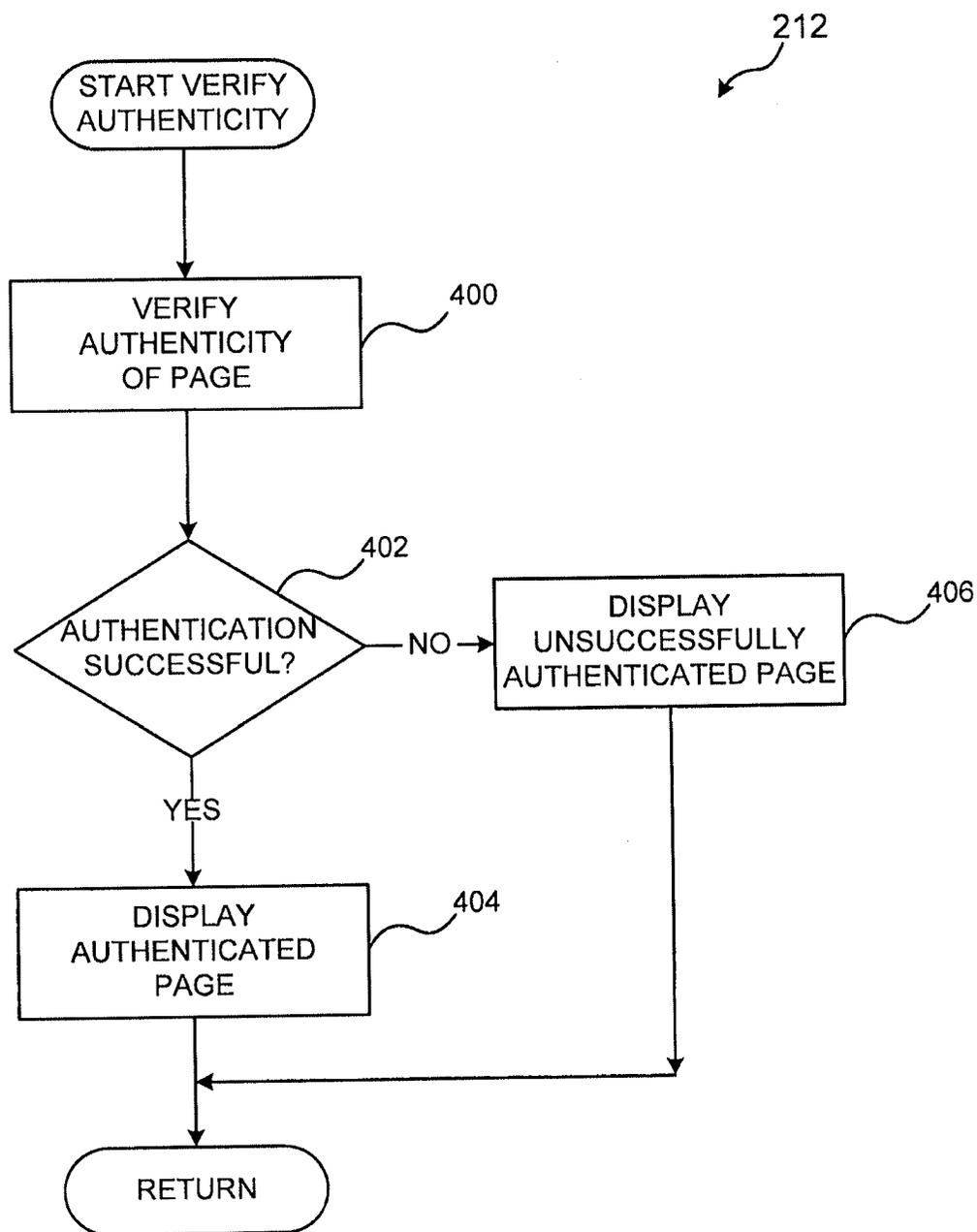


FIG. 8

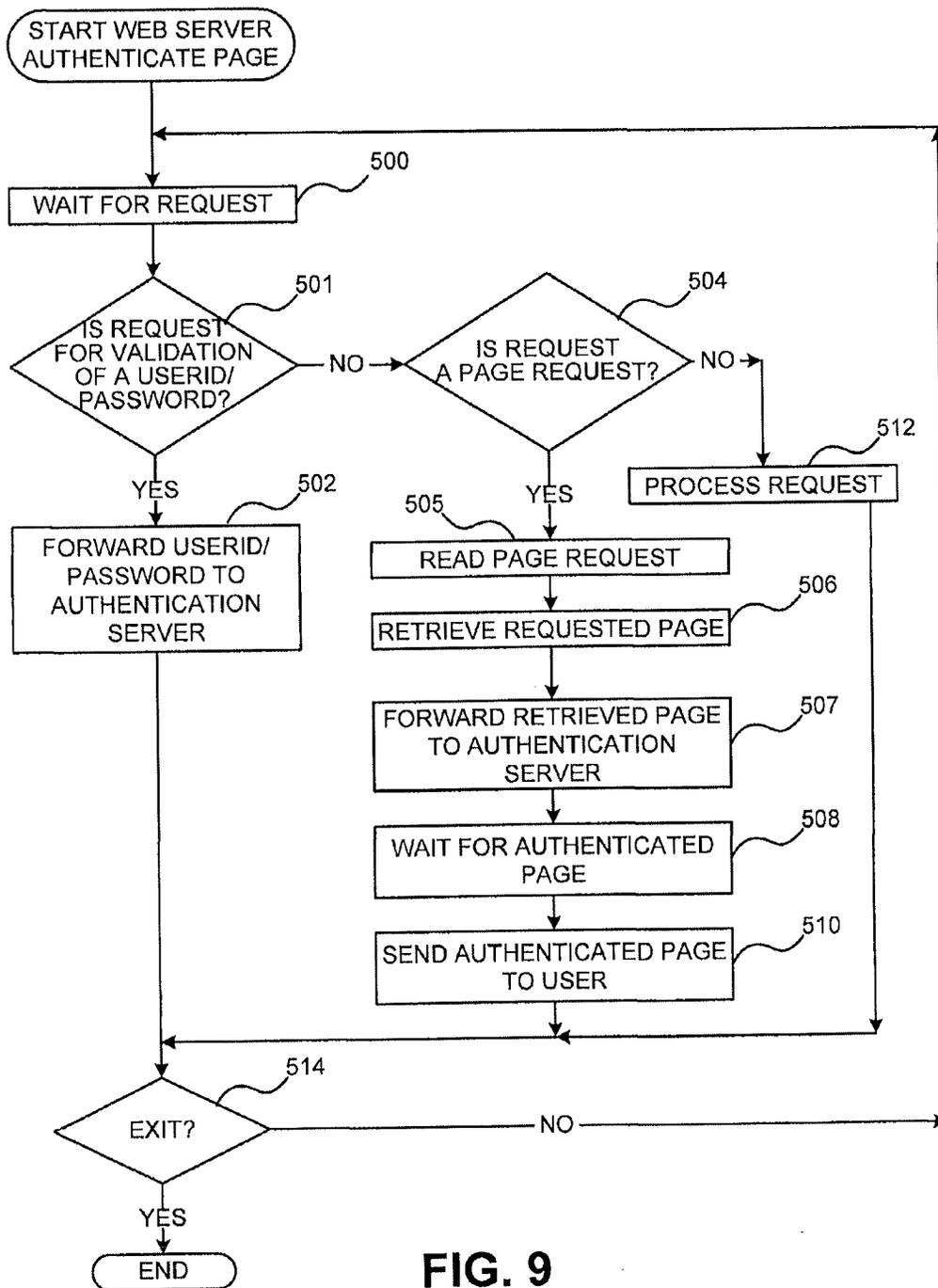


FIG. 9

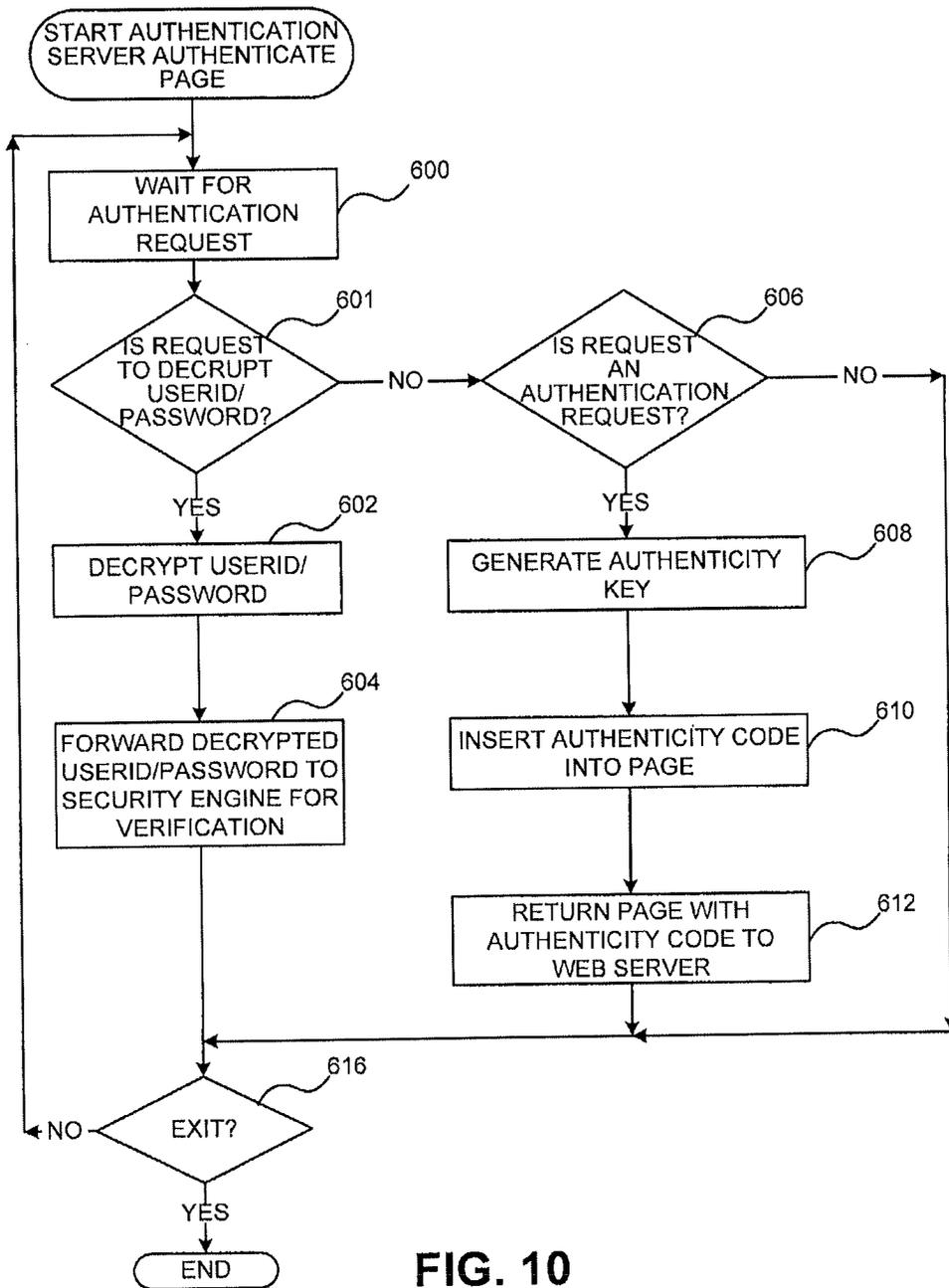


FIG. 10

U.S. Patent

Dec. 8, 2009

Sheet 12 of 12

US 7,631,191 B2

```
<OBJECT ID="Checker" CLASSID="CLSID:B2157787-7492-11D4-8296-00609430A416"  
CODEBASE="APge.dll"  
SIGN="Tud9LuaH9v5QMqcHGUAmtDNhvZ3nGtUEHUMiGIsORV8v7JF9fp  
IBiq3Jod0SvdCqQxq+4DzXc  
SDK+5r6dbpJMTKiZQWLJpwNJJuJSS+cfywEXdQHxcOpRt8Hryl833Bg41s  
AIT+SCg5j7DBlzsvIVwohe  
chGYv5476AOavkoJrD4="></OBJECT>
```

FIG. 11

Appx87

US 7,631,191 B2

1

**SYSTEM AND METHOD FOR
AUTHENTICATING A WEB PAGE****CROSS-REFERENCE TO RELATED
APPLICATIONS**

This application is a continuation of and claims priority to U.S. application Ser. No. 09/656,074 filed on Sep. 6, 2000, which application is a non-provisional of and claims priority to U.S. Provisional Application No. 60/153,004, filed Sep. 9, 1999, the entire contents of which are hereby incorporated by reference.

FIELD OF THE INVENTION

The present invention relates generally to computer security, and more particularly, to systems and methods for authenticating a web page.

BACKGROUND OF THE INVENTION

Web pages often include icons, such as, corporate logos, patterns, characters, symbols or other indicators, that a user associates with a particular offering in the real world. A trust or good will is often associated with the recognition of a given set of icons. These icons are implemented, for example, as bitmaps, but unfortunately, these bitmaps can be copied and used to defraud a prospective customer. Additionally, customers rely on the accuracy of a URL of a web page. However, it is relatively easy for a "fraudster" to register a URL that is like the one the user is expecting, but is not quite the same. For example, "www.bigbank.com" vs. "www.bigbank.com" (with an "l" instead of an "i"). Thus, a user may retrieve an unwanted webpage that appears authentic. Therefore, the user may not always be confident that the web page being viewed is authentic and the true owner of a web page may be uncertain.

In addition to a user's lack of confidence in the true owner of a web page, there currently exists a problem (either real or perceived) in the transport of UserIDs/Passwords across the Internet. While most sites provide security, for example by using a secure protocol such as Secure Hypertext Transfer Protocol (HTTPS) for sensitive data, most consumers are complacent about checking for this security. Thus, a need exists for a system and method that allow a page to be authenticated so that a user feels secure in the authenticity of pages displayed from Internet sites.

SUMMARY OF THE INVENTION

In exemplary embodiments of the invention, a user requests a web page from a web site using a web browser. The web server receives the request, retrieves the web page and forwards it to an authentication server. The authentication server inserts an authenticity key into the web page, then the page (including the authenticity key) is returned to the user. If the page includes an authenticity key, the authenticity is verified at the user's computer because the user computer includes logic (e.g., software) to verify the authenticity.

In exemplary embodiments, the authenticity verification software is a browser plug-in and is configured by the user after it is downloaded to the user's computer. During the user configuration process, the user defines an authenticity stamp which determines the format of an authenticated page. In alternative embodiments, the user defines a non-authenticity stamp which will appear on non-authenticated pages.

2

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features and advantages of the present invention are hereinafter described in the following detailed description of illustrative embodiments to be read in conjunction with the accompanying drawing figures, wherein like reference numerals are used to identify the same or similar parts in the similar views, and:

FIG. 1 is an exemplary web page that has not been authenticated;

FIG. 2 is the exemplary web page of FIG. 1 that has been authenticated in accordance with the present invention;

FIG. 3 is the exemplary web page of FIG. 1 that has been authenticated using an alternative embodiment of the present invention;

FIG. 4 is a block diagram of an exemplary system configuration suitable for implementing the present invention;

FIG. 5 is a message sequence diagram for performing page authentication in accordance with the present invention;

FIGS. 6A and 6B are a flow diagram illustrating exemplary logic performed by a user computer for performing authentication in accordance with the present invention;

FIG. 7 is a flow diagram illustrating exemplary logic for loading an authentication module in accordance with the present invention;

FIG. 8 is a flow diagram illustrating exemplary logic for verifying authenticity and displaying an authenticated page in accordance with the present invention;

FIG. 9 is a flow diagram illustrating exemplary logic performed by a web server for performing authentication in accordance with the present invention;

FIG. 10 is a flow diagram illustrating exemplary logic performed by an authentication server in accordance with the present invention; and

FIG. 11 is an exemplary authenticity key.

DETAILED DESCRIPTION

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 of the icon and is not merely a copy. In various exemplary embodiments of the invention, a hierarchy of validations exists which allow not only for the validation of an individual icon, but also for the validation of screens and Uniform Resource Locators (URLs). Unlike Secure Sockets Layer (SSL) or other "security session" protocols, the present invention validates aspects of the screen display independent of the communications channel between the user and the web site (however, security session protocols may be used in addition to the present invention). The validation is performed using only information that the true owner of the icon can possess.

FIG. 1 is an example of a simple web page. The web page includes a title 52, several hyperlinks 54A, 54B, 54C and 54D, some textual information 56 and two graphical images 58A and 58B.

A web page that has been authenticated using the present invention will include all of the information in the same format as the non-authenticated page. As shown in FIG. 2, in addition to the information that would normally be displayed, an authenticated page includes an authenticity stamp 60 in which the user can specify the appearance of the authenticity stamp. For example, the user of the example shown in FIG. 2 defined the authenticity stamps to be a diamond shape which includes text (bold and italicized) that states "JOE'S SEAL OF APPROVAL." It will be appreciated that an unlimited

US 7,631,191 B2

3

number of variations of an authenticity stamp are possible. A user can configure the stamp to be graphics only, text only or a combination thereof. The user also specifies the color and other attributes of the stamp, for example, a blinking stamp. The user also specifies the location of the stamp, e.g., bottom right corner of the web page, pop-up dialog box, etc. In exemplary embodiments, the authenticity stamp can be audio instead of or in addition to visual. In alternative embodiments, a non-authenticated page is stamped and an authenticated page is not stamped. For example, the stamp is configured to be a red, flashing icon that reads "PAGE NOT AUTHENTICATED" in the upper right-hand corner, while a page that is authenticated does not include this stamp. In alternative examples, the user can define both an authenticity stamp and a non-authenticity stamp.

FIG. 3 illustrates an alternative embodiment wherein each graphical image includes an embedded authenticity stamp 62A and 62B. In the example illustrated in FIG. 3, each graphical element has an authenticity stamp containing the text "A-OKAY" embedded in the graphical image. In exemplary embodiments, the authenticity stamp is defined by the user. In other embodiments, the authenticity stamp is defined by the owner of the page being displayed (e.g., the web server). In such embodiments, the stamp can include the name of the trusted entity (i.e., the true owner of the page).

FIG. 4 is a block diagram of an exemplary environment 100 suitable for implementing the present invention. The system 100 includes one or more clients (e.g., users) 110 that communicate with one or more servers (e.g., web servers) 120. The users 110 can use any type of computing device that includes a display device, for example, a Personal Computer. It will be appreciated that other computing devices can be used, for example, a Personal Digital Assistant (PDA), a hand-held computing device, a cellular telephone, etc. The web server can be any site, for example a commercial web site, such as a merchant site, a government site, an educational site, etc. The user 110 establishes a connection to the web server 120 via a network 130, such as the Internet. The user 110 and web server 120 can communicate using a secure protocol (e.g., HTTPS) or a non-secure protocol (e.g., HTTP). The user 110 requests information from the web server 120, and in exemplary embodiments, the information is communicated using web pages, for example using Hyper-Text Markup Language (HTML). The web pages are displayed on the user's computer 110, for example, using a browser, such as, Netscape Communicator available from the Netscape Corporation of Mountain View, Calif. or Internet Explorer available from the Microsoft Corporation of Redmond, Wash. Prior to sending the requested web page to user 110, web server 120 submits the information to authentication server 140 where authenticating information is added. The information which includes the authenticating information is returned to the web server 120 which then sends the web page including the authentication information to the user 110.

In various exemplary embodiments, the authentication server 140 communicates with a security engine 150, for example to verify UserID/Password logons or single use passwords or identifiers. In exemplary embodiments, the security engine 150 is a commercially available security engine, such as, Siteminder available from Netegrity Corporation, of Waltham, Mass.

The examples illustrated and described herein are directed to exemplary embodiments in which a user utilizes a web browser to request web pages from a web server. However, it will be appreciated that various embodiments are possible wherein a client (e.g., web browser) requests content (e.g., a

4

web page) from a server (e.g., a web server). The present invention allows the server to provide the client with assurance as to the authenticity of the content (e.g., assure the client as to the true owner of the content).

FIG. 5 is a message sequence diagram illustrating exemplary communications among various components to assure a user of the authenticity of a page. User 110 includes a web browser 112 and a plug-in 114. A user requests a page 180, but the user (e.g., user computer) 110 has no knowledge that the page requested is "special" (e.g., is subject to page authentication). Thus, the page request 180 is a normal page request (e.g., a HTTP or HTTPS request for a page).

The web server 120 receiving the page request 180 determines whether the request is for an authenticated page. If the page is to be authenticated, the page is dynamically signed with a private key and additional information, such as a salt with a time stamp is also included as described in further detail later. The signed page is returned with a special authenticated page MIME type and returned to the web browser 112. Based on the MIME type, the web browser activates the appropriate plug-in 114.

The plug-in 114 uses a public key to verify the signature, and upon verification of the signature, the plug-in can validate the authenticity of the page. The plug-in 114 requests the user's preferences key 186 so that the page can be displayed with an authenticity stamp. In exemplary embodiments, the request for preferences key includes a shared secret and is encrypted with the public key and salt. Upon receipt of the request for preferences key 186, the web server 120 decrypts the request using the private key, validates the shared secret and encrypts the preferences key with the private key, shared secret and salt from the request 186. The encrypted preferences key is then returned to the plug-in 114.

The plug-in 114 reads the preferences file and decrypts it using the preferences key from the web server 120. In exemplary embodiments, the preferences file is stored on the user's 110 file system. However, the location of the file is not readily known to the plug-in 114. Thus, the plug-in 114 must get the preferences key to determine the location of the preferences file. The plug-in 114 reads the preferences file to determine the authenticity stamp and how it is to be displayed. The page is then displayed with the user's preferred authenticity stamp 190.

FIGS. 6A-10 illustrate exemplary logic for performing page authentication in accordance with the present invention. The flow diagrams illustrate in further detail the logic illustrated in the message sequence diagram of FIG. 5. In addition to authenticating a page, the present invention provides for additional security wherein a UserID/Password are encrypted with the public key to prevent "man in the middle" attacks. FIGS. 6A-8 illustrate exemplary logic performed by a user computer 110 as described below. FIG. 9 illustrates exemplary logic performed by a web server 120 as described below. FIG. 10 illustrates exemplary logic performed by an authentication server 140 as described below. It will be appreciated that various configurations are possible. For example, the logic of the authentication server 140 can be combined with the logic of the web server 120.

FIGS. 6A and 6B are a flow diagram illustrating exemplary logic performed by a user 110 for performing authentication in accordance with the present invention. The logic described herein is directed to web pages, however it will be appreciated that the information requested can be of various formats. The logic of FIG. 6A moves from a start block to block 200 to wait for a page request. It will be appreciated that a page request is known in the art, for example, a user enters a Uniform Resource Locator (URL) or clicks on a hyperlink. The logic

US 7,631,191 B2

5

then moves to block 201 where a received page request is sent to a web Server 120 to retrieve the requested page. The logic then moves to block 202 where the user (e.g., the user's browser) waits for the requested page. The logic of retrieving and formatting the requested page is described below with reference to FIGS. 9 and 10. When the requested page is received, the logic moves to block 204 where the page is read.

After a page is read, the logic moves to decision block 205 where a test is made to determine if a UserID/Password is required. It will be appreciated that a UserID/Password may be required for both pages requiring authentication and pages not requiring authentication. If a UserID/Password is required, the logic moves to block 206 where a UserID/Password is obtained. If a UserID/Password is required, a suitable logon screen is displayed on the user's computer. The UserID/Password entry display can be of varying formats, for example, a web page or a pop-up dialog box. Upon entry of a UserID/Password, the user indicates completion (for example, by pressing an "OK" or "Submit" button). Upon completion of the logon, the logic moves to block 207 where the UserID/Password is encrypted to prevent man in the middle attacks. The logic then moves to block 208 where the encrypted UserID/Password is sent to the web Server.

If a UserID/Password is not required, the logic moves to decision block 209 (FIG. 6B) where a test is made to determine if authentication is required. In exemplary embodiments, an authenticity key will be hidden in any page that should be authenticated. In order to determine if the page should be authenticated, the page source is read to determine if an authenticity key is included in the page. If authentication is not required, the logic moves to block 210 where the non-authenticated page is displayed. A non-authenticated page is a traditional web page (i.e., the way the web page would be displayed without the authentication of the present invention, such as the example shown in FIG. 1).

If authentication is required (yes in decision block 209), the logic moves to decision block 211 where a test is made to determine if the authentication module is loaded. In exemplary embodiments, the authentication module is a plug-in module for the web browser. In exemplary embodiments, if the authentication module has not been loaded, a message will be displayed. For example, "This page protected by AuthentiPage, to get a free copy, go to AuthentiPage.com." Alternatively, the message may ask the user if a download of the authentication module is desired. If the authentication module is not loaded, the logic moves to decision block 214 where a test is made to determine if the authentication module should be loaded. If the authentication module is not to be loaded, the logic moves to block 218 where the page is displayed without authentication. In exemplary embodiments, the user will be notified that the page could not be authenticated, for example via a pop-up window displaying a warning message. In alternative embodiments, the user defines a non-authenticity stamp which is displayed for a page that has not been authenticated.

If the authentication module is to be loaded (yes in decision block 214), the logic moves to block 216 where the authentication module is loaded as shown in FIG. 7 and described next. If a download of the authentication module is desired, the user may be automatically redirected to the download site.

FIG. 7 illustrates exemplary logic for loading an authentication module (block 216 of FIG. 6B). The logic of FIG. 7 moves from a start block to block 300 where the authentication module (e.g., plug-in) is downloaded. The download is accomplished using techniques known in the art. After the authentication module is downloaded to the user's computer, the logic moves to block 302 where the authentication module

6

is configured. As part of the configuration process, an authenticity stamp is defined by the user. This authenticity stamp will be displayed whenever an authenticated page is loaded. The stamp can take several forms, for example, a user-selected keyword, color, etc. Preferably, the determination of the look of the authenticity stamp is under complete control of the user. Preferably, the user is also able to determine where the stamp will be displayed, for example in a separate pop-up box or in a selected area of the web page. By requiring the user to configure the visual qualities of the stamp, the possibility of a counterfeit stamp being displayed is reduced. The user will expect to see his or her stamp and will begin to associate the stamp with security. It will be appreciated that while the stamp is defined in terms of visual qualities herein, embodiments of the invention can include defining the stamp in other ways, for example, by an audio indication specified by the user. After the authentication module has been configured, the logic of FIG. 7 ends and processing returns to FIG. 6B.

Returning to FIG. 6B, after the authentication module is loaded (block 216), or if it has been determined that the authentication module is already loaded (yes in decision block 211), the logic moves to block 212 to verify the authenticity of the page and display the page, as shown in detail in FIG. 8 and described next.

FIG. 8 illustrates exemplary logic for verifying the authenticity of a page and displaying the page. The logic of FIG. 8 moves from a start block to block 400 where the authenticity of the page is verified. Many algorithms can be used to verify the authenticity. For example, the trusted server that generates the authenticity key can encrypt the authenticity key with a private key. The user can then decrypt the authenticity key using a public key. Using this method, no certificate is required and no interaction is required by the user. Other algorithms can be used, some of which may require a certificate and/or user interaction. Unless the page contains confidential information, the authentication of pages should not require any additional security or encryption. The authentication of a page can be employed on any page, for example, marketing data, purchase information, etc., to prove the page's authenticity. In general, authentication of pages will not require additional security or encryption. However, if additional security is desired, page authentication performed in accordance with the present invention can be used in combination with other known or future security measures, for example, in conjunction with a secure protocol, such as HTTPS, along with the requirement for a UserID and a password, etc. If the authentication is successful (yes in decision block 402), the logic moves to block 404 where the page is displayed with the authenticity stamp as defined by the user during the configuration process described above. If the authentication fails (no in decision block 402), the logic moves to block 406 where the unsuccessfully authenticated page is displayed. In exemplary embodiments, an indication of the authentication failure is provided, for example a warning message may be displayed. For example, a flashing error message, such as "PAGE NOT AUTHENTICATED" can be displayed in the location where the authenticity stamp would normally be displayed. After the page is displayed (either as an authenticated page in block 404 or as an unsuccessfully authenticated page in block 406), the logic of FIG. 8 ends and processing returns to FIG. 6B.

Returning to FIG. 6B, after a page has been displayed (block 210, 212 or 218) or a UserID/Password request has been processed, the logic moves to decision block 220 (FIG. 6A) where a test is made to determine if it is time to exit. For example, if the user selects an "Exit" option from a web browser menu, it is time to exit. If it is not time to exit, the

US 7,631,191 B2

7

logic returns to block 200 to wait for the user's next page request. The logic of blocks 200-220 is repeated until it is time to exit. It will be appreciated that in alternative embodiments of the invention requests other than those shown and described herein may also be processed. When it is time to exit, the logic of FIG. 6A ends.

FIG. 9 is a flow diagram illustrating exemplary logic performed by a web server 120 for performing authentication in accordance with the present invention. The logic of FIG. 9 moves from a start block to block 500 where the web server waits for a request. In exemplary embodiments, while the web server is waiting for a request other requests continue to be serviced (e.g., receiving and processing page requests). When a request is received, the logic moves to decision block 501 where a test is made to determine if the request is a request for validation of a UserID/Password. If so, the logic moves to block 502 where the received UserID/Password (sent in block 108 of FIG. 6A) is forwarded to the authentication server 140.

If the request is not a request for verification of a UserID/Password, the logic moves to decision block 504 where a test is made to determine if the request is a page request. If so, the logic moves to block 505 where the page request is read. The logic then moves to block 506 where the requested page is retrieved. Next, the logic moves to block 507 where the requested page is forwarded to an authentication server 140. The logic then moves to block 508 where the web server waits for the authenticated page to be returned from the authentication server. In exemplary embodiments, while the web server is waiting for an authenticated page, other processing can be performed, for example, page requests can be received and processed. When an authenticated page is received, the logic moves to block 510 where the authenticated page is returned to the user that requested the page.

If the request is not a request to verify a UserID/Password (no in decision block 501) or a page request (no in decision block 504), the request is another request, which is processed in block 512. Other requests which may be processed by a web Server are not described herein.

After the request (e.g., request for verification of UserID/Password, page request or other request) has been processed, the logic moves to decision block 514 where a test is made to determine if it is time to exit. The logic of blocks 500-514 is repeated until it is time to exit (e.g., shut down the web server). When it is time to exit, the logic of FIG. 9 ends.

FIG. 10 is a flow diagram illustrating exemplary logic performed by an authentication server 140 for performing authentication in accordance with the present invention. The logic of FIG. 10 moves from a start block to block 600 where the authentication server waits for an authentication request. When an authentication request is received, the logic moves to decision block 601 to determine if the request is a request to decrypt a UserID/Password. If so, the logic moves to block 602 where the UserID/Password is decrypted. The logic then moves to block 604 where the decrypted UserID/Password is forwarded to a security engine for verification. In exemplary embodiments, the security engine is an existing security engine, such as a DSS Security Engine. The Security Engine verifies the UserID/Password and forwards the verification as appropriate. For example, if the UserID is not valid, a message will be displayed on the user's computer. Because security engines are known in the art, the logic employed by the security engine is not discussed further herein.

If the request is not a request to decrypt a UserID/Password, the logic moves to decision block 606 where a test is made to determine if the request is an authentication request. If so, the logic moves to block 608 where the authentication server generates an authenticity key. Details for an exemplary

8

authenticity key are described below. The logic of FIG. 10 then moves to block 610 where the authenticity key is inserted into the web page. An exemplary authenticity key is shown in FIG. 12. Next, the logic moves to block 612 where the page which includes the authenticity key is returned to the web server.

While the exemplary embodiments only include processing of requests for encryption/decryption or authenticating a page, it will be appreciated that alternative embodiments may process other requests. After a request is processed (e.g., a UserID/Password is decrypted or a page is authenticated), the logic moves to decision block 616 where a test is made to determine if it is time to exit. The logic of blocks 600-616 is repeated until it is time to exit (e.g., shut down the authentication server). When it is time to exit, the logic of FIG. 10 ends.

In alternative embodiments, there is no authentication server. Rather, graphical images include a hidden identifier identifying the true owner, as well as a cryptographic signature to ensure that the graphical image cannot be tampered with by a counterfeiter. In various embodiments, the identification is a portion of a URL that is encrypted, such as "bigbank.com". Those skilled in the art will recognize this as a second-level domain name. Upon receipt of the web page, the authentication module residing on the user's computer compares the identification in the page with the URL from which the web page was fetched. If the identification matches, the web page was served by its true owner. If the identifications do not match, the user is provided with an indication that the URL is not the true owner of the graphical images. For example, a "counterfeit" site may look just like the site that it was intended to look like because the counterfeiter can copy the page, including the graphical images. However, if the graphical images include a hidden identifier, the user can be notified that the page is "counterfeit."

An exemplary authenticity key is constructed in such a way that "freshness" can be determined, for example using a date/time stamp. The authenticity key will also include other identifying information as described later. An exemplary authenticity key contains one or more hidden signature objects. In exemplary embodiments, the hidden signature object is a value that is the encoding of the following fields: web page hash, action, date/time, key identifier and digital signature. In exemplary embodiments, the web page hash is generated using SHA-1 on the entire web page excluding this hidden signature object. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST) and is specified in the Secure Hash Standard (SHS, FIPS 180). SHA-1 is a revision to SHA that was published in 1994. SHA-1 is also described in the ANSI X9.30 (part 2) standard. The algorithm takes a message of greater than 264 bits in length and produces a 160-bit message digest.

The action is a value used to specify the action to be performed by the browser plug-in that verifies this page. Preferably, if the user computer does not have the browser plug-in installed, the user will be informed of the required plug-in. Preferably, the user can elect to download the plug-in at the time the web page is received, in which case the web page can be displayed immediately after installing the plug-in. In exemplary embodiments if the user elects not to install the plug-in, the web page is displayed and the user is provided with an indication (e.g., a warning message displayed in a pop-up window) that the page was not authenticated. Actions are specified in a bit-wise manner so that multiple actions can be specified. For example, the action value may be defined to both display the security object (e.g., to display a bitmapped image) and to request a secure login.

US 7,631,191 B2

9

The date/time field is used to specify the current date and time that the web page was delivered from the web server. This value is used by the browser plug-in to verify that the page is "fresh" (e.g., is not being replayed by a rogue site). The present invention may include a synchronization feature which allows the user's computer to synchronize its internal clock with atomic clocks available over the Internet. This would provide additional security by allowing a more precise verification of the date/time stamp.

The key identifier is used to identify the public key used to verify the signature. In exemplary embodiments, a digital signature is used as a salt value concatenated with an SHA-1 hash of the other four fields (web page hash, action, date/time and key identifier) that has been encrypted using the private key of the web Page server. A "salt value" is an arbitrary random value that constantly changes in order to minimize the possibility of various attacks.

In exemplary embodiments of the present invention, four keys are used in the web page authentication process: a private key, a public key, a master encryption key and a preferences encryption key. A private key (of the web page server) is used to create the "digital signature" within the web page signature. A digital signature is generally defined to include a certificate. For the purposes of the present invention, exemplary embodiments do not include a certificate. It will be appreciated that various embodiments can include a certificate in the digital signature. The private key is only distributed to applications requiring its use. A public key is buried in multiple pieces throughout the browser plug-in. The public key is used to verify the Digital Signature within the web Page signature. Although the public key itself can be distributed, its storage location should remain as obscure as possible to reduce the possibility of attacks. The master encryption key is also buried in multiple places in the browser plug-in. The master encryption key is used to encrypt the preferences encryption key that is stored on the user's computer. The preferences encryption key that is stored on the user's computer is used to encrypt preferences (e.g., user configuration information, such as appearance and location of authenticity stamp) that are stored on the user's computer.

When the action indicates a Login, the browser plug-in displays a user ID and password request on the user's computer along with the secure word that will authenticate the UserID and Password request. These two values will be prefixed with the salt value and date/time information from the web page signature and encrypted using the public key. This information will then be sent by the plug-in performing the Submit. Preferably, the Submit explicitly references the URL to which the information is to be sent. This will allow the information only to be sent to the destination that was previously signed within the web Page signature.

The preferences file is used to store information, such as a user's secure word. Preferably, the preferences file is placed in a random directory to help obscure the location of the preference file and facilitate the creation of unique user configurations. This increases the difficulty in creating a general purpose rogue program for extracting preferences and keys.

In exemplary embodiments, new keys are implemented through redistribution of the browser plug-in. The new plug-in can contain both the old and new keys to facilitate implementation of the new keys on a particular date.

In exemplary embodiments of the invention, the authentication module may contain a list of all known UserIDs. The list of known UserIDs can be displayed so that the user can select a desired UserID. Upon selection of a UserID, the user is prompted to enter a password. The UserID and password are encrypted with the use of the public key to authenticate the

10

authenticity key. The entire string (e.g., [UserID][Password][original salt value]) is sent to the trusted server for verification. The trusted server 120 then extracts the UserID and password and forwards them to the authentication server 140 for verification.

Exemplary embodiments allow a user to check the validity of their authentication module. A server allows the authentication module to send a request for self-verification. In various embodiments, the validation is performed in response to a user request. In exemplary embodiments, the authentication module includes a suitable user interface which allows a user to request self-verification. The authentication module generates a random number ("salt") and encrypts it with the public key. The value is then sent to a known URL (e.g., a URL that is hard-coded in the authentication module). When the authentication module receives the request, it is decrypted using the private key and adding an additional salt value which is then returned to the client module (user). The client module decrypts the response received from the authentication module. The random values are then compared (without the additional salt added by the authentication module). If the value matches the value originally sent, the self-verification is successful. A verification result is displayed to the user to indicate whether the verification was successful.

The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware and/or software components configured to perform the specified functions. For example, the present invention may employ various integrated circuit components, e.g., memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more microprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, or the like, with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction of cryptography, please review a text written by Bruce Schneier which is entitled "Applied Cryptography: Protocols, Algorithms, And Source Code In C," published by John Wiley & Sons (second edition, 1996), which is hereby incorporated by reference.

It should be appreciated that the particular implementations shown and described herein are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data networking, application development and other functional aspects of the systems (and components of the individual operating components of the systems) may not be described in detail herein. Furthermore, the connecting lines shown in the various figures contained herein are intended to represent exemplary functional relationships and/or physical couplings between the various elements. It should be noted that many alternative or additional functional relationships or physical connections may be present in a practical electronic transaction system.

To simplify the description of the exemplary embodiments, the invention is frequently described as pertaining to an authentication system. It will be appreciated, however, that many applications of the present invention could be formulated. One skilled in the art will appreciate that the network

US 7,631,191 B2

11

may include any system for exchanging data or transacting business, such as the Internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. The users may interact with the system via any input device such as a keyboard, mouse, kiosk, personal digital assistant, handheld computer (e.g., Palm Pilot®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, workstation, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, or the like. Moreover, although the invention is frequently described herein as being implemented with TCP/IP communications protocols, it will be readily understood that the invention could also be implemented using IPX, Appletalk, IP-6, NetBIOS, OSI or any number of existing or future protocols. Moreover, while the exemplary embodiment will be described as an authentication system, the system contemplates the use, sale or distribution of any goods, services or information over any network having similar functionality described herein.

The customer and merchant may represent individual people, entities, or business. The bank may represent other types of card issuing institutions, such as credit card companies, card sponsoring companies, or third party issuers under contract with financial institutions. It is further noted that other participants may be involved in some phases of the transaction, such as an intermediary settlement institution, but these participants are not shown.

Each participant is equipped with a computing system to facilitate online commerce transactions. The customer has a computing unit in the form of a personal computer, although other types of computing units may be used including laptops, notebooks, hand held computers, set-top boxes, and the like. The merchant has a computing unit implemented in the form of a computer-server, although other implementations are possible. The bank has a computing center shown as a main frame computer. However, the bank computing center may be implemented in other forms, such as a mini-computer, a PC server, a network set of computers, and the like.

The computing units are connected with each other via a data communication network. The network is a public network and assumed to be insecure and open to eavesdroppers. In the illustrated implementation, the network is embodied as the internet. In this context, the computers may or may not be connected to the internet at all times. For instance, the customer computer may employ a modem to occasionally connect to the internet, whereas the bank computing center might maintain a permanent connection to the internet. It is noted that the network may be implemented as other types of networks, such as an interactive television (ITV) network.

Any merchant computer and bank computer are interconnected via a second network, referred to as a payment network. The payment network represents existing proprietary networks that presently accommodate transactions for credit cards, debit cards, and other types of financial/banking cards. The payment network is a closed network that is assumed to be secure from eavesdroppers. Examples of the payment network include the American Express®, VisaNet® and the Veriphone® network. In an exemplary embodiment, the electronic commerce system is implemented at the customer and issuing bank. In an exemplary implementation, the electronic commerce system is implemented as computer software modules loaded onto the customer computer and the banking computing center. The merchant computer does not require any additional software to participate in the online commerce transactions supported by the online commerce system.

12

The corresponding structures, materials, acts and equivalents of all elements in the claims below are intended to include any structure, material or acts for performing the functions in combination with other claimed elements as specifically claimed. The scope of the invention should be determined by the allowed claims and their legal equivalents, rather than by the examples given above.

The invention claimed is:

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 (i) to enable the authenticity key to be retrieved from the formatted data and (ii) to locate a preferences file, wherein an authenticity stamp is retrieved from the preferences file.

2. The method of claim 1, wherein the formatted data is a web page.

3. The method of claim 1, further comprising: reading the formatted data; and, verifying authenticity of the formatted data based on the authenticity key in response to the formatted data including the authenticity key.

4. The method of claim 3, further comprising displaying the formatted data in response to the verification of the authenticity key.

5. The method of claim 3, wherein the authenticity stamp is displayed for formatted data that is verified.

6. The method of claim 3, wherein the authenticity stamp is displayed for a graphical image within the formatted data.

7. The method of claim 3, wherein a non-authenticity stamp is displayed for formatted data that is not verified.

8. The method of claim 1, wherein the formatted data is at least one of: a screen display or a Uniform Resource Locator (URL).

9. The method of claim 1, further comprising receiving third party data.

10. The method of claim 1, further transforming received data by inserting a second authenticity key into the received data.

11. The method of claim 1, wherein the authenticity key is received from a third-party.

12. The method of claim 1, further comprising retrieving additional data based on the received data.

13. The method of claim 1, further comprising validating the formatted data based on the authenticity key and, further transforming by inserting a second authenticity key into the formatted data.

14. The method of claim 1, further comprising retrieving an image selection based on a selection from a plurality of images, wherein the plurality of images are only known by a client and a challenge server.

15. The method of claim 14, wherein the image selection is at least one of: a graphic, text, video, or audio.

16. The method of claim 1, wherein the returning includes returning the formatted data to at least one of: a Personal Computer (PC), Personal Digital Assistant (PDA), cellular telephone, or an email device.

17. An authentication system comprising: an authentication processor configured to insert an authenticity key into formatted data to enable authentication of the authenticity key (i) to verify a source of the formatted data and (ii) to retrieve an authenticity stamp from a preferences file.

US 7,631,191 B2

13

18. The system of claim 17, wherein the formatted data is displayed on a client.

19. The system of claim 17, wherein the authentication processor is further configured to send the formatted data including the authenticity key to a client.

20. The system of claim 19, wherein authenticity of the formatted data is verified based on the authenticity key.

21. The system of claim 20, wherein the formatted data is displayed with an indication of the authenticity of the formatted data.

22. The system of claim 17, wherein the authentication processor is further configured to receive the formatted data from a third party.

23. The system of claim 17, wherein 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.

24. The system of claim 17, wherein the authentication processor is further configured to receive a preferences key from a third party.

25. The system of claim 17, wherein the authentication processor is further configured to receive additional data based the formatted data.

26. The system of claim 17, wherein the authentication processor is further configured to validate the formatted data based on the authenticity key and, to insert a second authenticity key into the formatted data.

27. The system of claim 17, wherein the authentication processor is further configured to receive an image selection that is at least one of: a graphic, text, video, or audio from the source based on a selection from a plurality of images, wherein the plurality of images are only known by a client and a challenge server.

14

28. The system of claim 17, wherein a client authenticates the authenticity key and the client is at least one of: a Personal Computer (PC), Personal Digital Assistant (PDA), cellular telephone, or an email device.

29. An authentication system comprising:
an authentication processor configured to send formatted data having an authenticity key to a client, wherein the authenticity key enables location of a preferences file, and wherein an authenticity stamp is retrieved from the preferences file.

30. The system of claim 29, wherein at least one of color or positioning of a graphic image within the formatted data is configurable.

31. A computer readable medium having stored thereon a plurality of instructions, the plurality of instructions comprising:

instructions to format received data by inserting an authenticity key to create formatted data; and
instructions to return the formatted data to a client, wherein the authenticity key is retrieved from the formatted data to locate a preferences file, and wherein an authenticity stamp is retrieved from the preferences file.

32. A method comprising:
receiving, at a client computer, formatted data from a authentication host computer wherein the authentication host computer receives the data to create received data, and transforms the received data by inserting an authenticity key to create the formatted data;
retrieving, by the client computer, the authenticity key from the formatted data to locate a preferences file; and
retrieving an authenticity stamp from the preferences file.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,631,191 B2
APPLICATION NO. : 11/423340
DATED : December 8, 2009
INVENTOR(S) : Glazer et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page item 76 the inventors' full addresses are inappropriately listed on the face of the patent. City, State and Country should be listed only.

Claim 1, column 12, line 14, "data (i) to" should be changed to --data to--; line 15, "and (ii) to" should be changed to --and to--.

Claim 10, column 12, line 41, "transforming received" should be changed to --transforming the received--.

Claim 13, column 12, line 50, "transforming by" should be changed to --transforming the received data by--.

Claim 16, column 12, line 60, "Computer (PC), Personal Digital Assistant (PDA), cellular" should be changed to --Computer (PC), a Personal Digital Assistant (PDA), a cellular--.

Claim 17, column 12, line 65, "key (i) to" should be changed to --key to--; line 66, "and (ii) to" should be changed to --and to--.

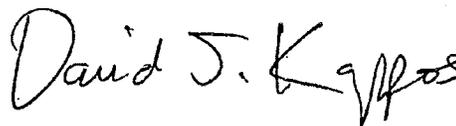
Claim 25, column 13, line 23, "based the" should be changed to --based on the--.

Claim 28, column 14, line 3, "Computer (PC), Personal Digital Assistant (PDA), cellular" should be changed to --Computer (PC), a Personal Digital Assistant (PDA), a cellular--.

Claim 32, column 14, lines 24 to 25, "from a authentication" should be changed to --from an authentication--.

Signed and Sealed this

Eleventh Day of May, 2010



David J. Kappos
Director of the United States Patent and Trademark Office

ADDENDUM C

157 Cong. Rec. S7413-02, 2011 WL 5526257
Congressional Record --- Senate
Proceedings and Debates of the 112th Congress, First Session
Monday, November 14, 2011

***S7413 BUSINESS-METHOD PATENTS**

Mr. KYL.

Mr. President, I ask unanimous consent to have printed in the

Record a letter concerning section 18 of the America Invents Act, sent to me and others by the chairman of the House Judiciary Committee.

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC September 8, 2011.

Hon.

Jon Kyl

U.S. Senate,
Washington, D.C.
Hon. CHARLES E. SCHUMER,
U.S. Senate,
Washington, D.C.
Hon. PATRICK LEAHY,
U.S. Senate,
Washington, D.C.
Hon. CHUCK GRASSLEY,
U.S. Senate,
Washington, D.C.

DEAR SENATORS KYL, SCHUMER, LEAHY AND GRASSLEY: I am writing to discuss further the importance of the transitional program for business method patents as included in H.R. 1249, the Leahy-Smith America Invents Act. As you know, this provision enables the U.S. Patent and Trademark Office ('USPTO') to correct egregious errors that were made in the granting of a wide range of business method patents.

Business methods were generally not patentable in the United States before the late 1990s, and generally are not patentable elsewhere in the world. The Federal Circuit, however, created this new class of patents in its 1998 State Street decision. In its 2010 decision in *Bilski v. Kappos*, the U.S. Supreme Court clamped down on the patenting of business methods and other patents of poor quality. It is likely that many or most of the business method patents that were issued after State Street are now invalid under *Bilski*.

There really is no sense in allowing expensive litigation over patents that are no longer valid in light of the Supreme Court's clarification of the law. The new transitional program included in the House bill creates an inexpensive and speedy alternative to litigation-allowing parties to resolve these disputes more efficiently rather than spending millions of dollars in litigation costs. In the process, the proceeding will also prevent nuisance litigation settlements.

Moreover, the new administrative proceeding allows business method patents to be reviewed by the experts at the USPTO under the correct (*Bilski*) standard. To use this proceeding, a challenger must make an up-front showing to the

USPTO of evidence that the business method patent is more likely than not invalid. This is a high standard. Only the worst patents, which probably never should have been issued, will be eligible for review in this proceeding.

This program provides the Patent Office with a fast, precise vehicle to review low-quality business method patents, which the Supreme Court has acknowledged are often abstract and overly broad.

Specifically, the bill's provision applies to patents that describe a series of steps used to conduct every-day business applications in the financial products and retail services sectors. These are patents that can be and have been asserted against all types of businesses—from community banks and credit unions to retailers and businesses of all sizes and from all industries.

The provision is, indeed, limited to patents that are non-technological in nature (i.e., business methods) and that involve a process or related apparatus used in the practice, administration, or management of a financial product or service. The program's exception for "technological inventions" precludes review of patents for inventions based on application of the natural sciences or related engineering or inventions in computer operations. And by requiring that the covered patents be applicable to a financial product or service, the proceeding in the House bill ensures that the patents eligible for review will generally include only those that have some business or commercial orientation.

Nothing in the bill, however, limits use of the proceeding to one industry; rather, it applies to non-technological patents that can apply to financial products or services. Any business that sells or purchases goods or services "practices" or "administers" a financial service by conducting such transactions. Most business-method patents are fairly plastic in nature and could apply to a whole host of business activities. See 157 Cong. Rec. 1363, 1365 (daily ed. March 8, 2011) (statement of Sen. Schumer) ("To meet this requirement, the patent need not recite a specific financial product or service. Rather the patent claims must only be broad enough to cover a financial product or service."). To be sure, the fact that a patent has been asserted against a financial institution with respect to products or processes that are unique to such institutions will be a fairly clear indicator that the patent applies to a "financial product or service," and should provide guidance to the USPTO in administering the program. See 157 Cong. Rec. 1368, 1379 (daily ed. March 8, 2011) (statement of Sen. Kyl).

The transitional program can be used to review patents for "a method or a corresponding apparatus." The distinction between a "process" and a "machine" (two of the terms used in section 101 of the patent code to define what is patentable) is not a firm one, and many inventions can be characterized either way. A "corresponding apparatus" for a business method would include, for example, a computer that was programmed to carry out the business process. Wary of the stigma that attaches to business-method patents, many applicants try to obscure the nature of these patents by characterizing a computer that has been programmed to execute the process as the invention, and thus asserting that the process is really a "machine" or a "system."

The program's definition of "covered business-method patent" includes a "corresponding apparatus" in order to prevent such obvious evasions. Any other approach would elevate claim-drafting form over invention substance. Finally, any "apparatus" that is subject to review under the program would need to be used to implement or effect a business method. Legitimate inventions in technological fields will not be subject to review under this program.

The transitional program also extends to prives of parties charged with infringement. This was done specifically to prevent downstream customers or users from being dragged into frivolous litigation over suspect or improperly granted patents. H.R. 1249 also extends the time frame for the transitional program. This change is important to prevent patent trolls from waiting out the program. This issue of folks "lying in wait" may actually be a significant argument for extending or making permanent this program in the future. Similarly, the program's definition was expanded in H.R. 1249 so that it is not limited to class 705 patents. This change is key to the program's success, because many business

method patents are assigned to classes other than 705, and it makes no sense to exclude them because of the quirks of USPTO's classification regime.

This program is not tied to one industry or sector of the economy-it affects everyone. The provision as developed in the Senate and later perfected in the House will ensure that the vast majority of non-technological business method patents will be eligible for review under this program. As the USPTO had a presumption to grant many of these erroneous patents, they should now have a presumption to allow most non-technological ***S7414** business method patents that have a commercial nexus into this new program for review. This program was designed to be construed as broadly as possible and as USPTO develops regulations to administer the program that must remain the goal.

The strength of our patent system relies on not simply the mechanical granting of a patent, but the granting of strong patents, ones that are truly novel and non-obvious inventions, that are true innovations and not the product of legal gamesmanship. This provision is an integral component of H.R. 1249 and will not only help correct past mistakes but ensure a stronger U.S. patent system going forward.

Sincerely,

LAMAR SMITH,
Chairman, Committee on the Judiciary,
House of Representatives.

End of Document

© 20 7 Thomson Reuters. No c a m to or g na U.S. Government Works.

CERTIFICATE OF SERVICE

I hereby certify that, on this 23rd day of March, 2017, I filed the foregoing Petition for Rehearing En Banc with the Clerk of the United States Court of Appeals for the Federal Circuit via the CM/ECF system, which will send notice of such filing to all registered CM/ECF users.

/s/ Robert T. Smith

Robert T. Smith

Counsel for Petitioners-Appellees