APPENDIX

APPENDIX

TABLE OF CONTENTS

APPENDIX A

NOTE: This disposition is nonprecedential.

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

2016-2415, 2017-2101, 2017-2191

[Filed September 11, 2018]

KAMRAN ASGHARI-KAMRANI,)
NADER ASGHARI-KAMRANI,)
Plaintiffs-Appellants)
)
v.)
)
UNITED SERVICES)
AUTOMOBILE ASSOCIATION,)
Defendant-Cross-Appellant)
)

Appeals from the United States District Court for the Eastern District of Virginia in No. 2:15-cv-00478-RGD-LRL, Senior Judge Robert G. Doumar.

JUDGMENT

ANTIGONE GABRIELLA PEYTON, Protorae Law PLLC, Tysons, VA, argued for plaintiffs-appellants. Also represented by REECE WERNER NIENSTADT, Nienstadt PLLC, Washington, DC.

AHMED JAMAL DAVIS, Fish & Richardson PC, Washington, DC, argued for defendant-cross-appellant. Also represented by MICHAEL T. ZOPPO, New York, NY; MATTHEW C. BERNTSEN, Boston, MA.

THIS CAUSE having been heard and considered, it is ORDERED and ADJUDGED:

PER CURIAM (DYK, WALLACH, and HUGHES, *Circuit Judges*).

AFFIRMED. See Fed. Cir. R. 36.

ENTERED BY ORDER OF THE COURT

September 11, 2018
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CIVIL NO. 2:15cv478

[Filed July 5, 2016]

NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI	)
Plaintiffs,	)
v.	)
UNITED SERVICES AUTOMOBILE ASSOCIATION	)
Defendant.	)

OPINION AND ORDER

This is a suit for patent infringement under 35 U.S.C. § 271. Second Am. Compl. ¶ 1, ECF No. 70. Plaintiffs Nader Asghari-Kamrani and Kamran Asghari-Kamrani ("Plaintiffs") have alleged that the United Services Automobile Association ("USAA" or "Defendant") has infringed several claims of United States Patent No. 8,266,432 ("the '432 patent"). Id. USAA has filed a Motion to Dismiss Plaintiffs' Second Amended Complaint. ECF No. 86. For the reasons set

forth below, the Court **GRANTS** the Motion to Dismiss, ECF No. 86, and **DISMISSES WITH PREJUDICE** Plaintiffs' Second Amended Complaint, ECF No. 70. The Court also **DISMISSES AS MOOT** USAA's Counterclaims. ECF No. 88.

I. BACKGROUND

A. PROCEDURAL HISTORY

On October 30, 2015, Plaintiffs filed their initial complaint for patent infringement pursuant to 35 U.S.C. § 271. Compl., ECF No. 1. On December 1, 2015, USAA filed a Motion to Dismiss for Failure to State a Claim. ECF No. 15. Before the Court heard argument on this Motion, Plaintiffs filed an Amended Complaint on December 21, 2015. ECF 19. USAA then filed a Motion to Dismiss for Failure to State a Claim on January 7, 2016. ECF No. 20. The Court granted this motion on the grounds that Plaintiffs had failed to plead with sufficient particularity. Order, ECF No. 60. The Court granted Plaintiffs leave to amend. Id. On April 12, 2016, Plaintiffs filed a Second Amended Complaint. ECF No. 70. On April 28, 2016, USAA filed the instant Motion to Dismiss. ECF No. 86. On May 12, 2016, Plaintiffs filed their Opposition to the Motion to Dismiss. ECF No. 101. On May 18, 2016, USAA filed its Reply. ECF No. 111. A hearing on the instant motion was held on June 27, 2016. ECF No. 137.

USAA moves for dismissal pursuant to Federal Rule of Civil Procedure 12(b) on two grounds: (1) because the claims of the '432 patent are directed to an abstract idea and are thus ineligible for patent protection; and (2) because the Second Amended Complaint fails to identify with sufficient particularity how USAA

infringes the patent. USAA's Mem. in Supp. of its Mot. to Dismiss ("USAA's Mem."), ECF No. 87 at 1. Because the Court holds that the patent is directed to patent-ineligible subject matter, it does not reach USAA's second contention.

B. PATENT-IN-SUIT

Plaintiffs allege that USAA infringes "at least claims 1-10, 12, 13, 16-26, 28-35, 38-42, 45, 47, 48, 50-52, 54, and 55" of the '432 patent. Second Am. Compl. ¶ 1. According to the Summary of the Invention, "[t]he invention relates to a system and method provided by a Central-Entity for centralized identification and authentication of users and their transactions to increase security in e-commerce." '432 patent 2:52–55, ECF No. 70-1, Ex. A. The patent identifies three entities that perform the patent's methods: (1) a "Central-Entity" which "centralizes user's personal and financial information in a secure environment in order to prevent the distribution of the user's information in e-commerce;" (2) a "user" which "represents both a typical person consuming goods and services as well as a business consuming goods and services, who needs to be identified in order to make online purchases or gain access to restricted web sites;" and (3) an "External-Entity" which "is any party offering goods or services in e-commerce and needs to authenticate the users based on digital identity." '432 patent at Summary of Invention, 2:56–3:6.

Initially, the user signs-up at the Central-Entity and provides his or her "personal or financial information." Id. at 3:7–8. The Central-Entity gives the user a UserName and Password that he or she will utilize when interacting with the Central-Entity. Id. at

3:8–13. When requested by the user, the Central-Entity also gives the user a SecureCode, which is "dynamic, nonpredictable and time-dependent." Id. at 3:13–16. The user may then provide his or her UserName and SecureCode to the External-Entity. Id. at 3:19–21. The External-Entity then sends the UserName and SecureCode to the Central-Entity, which will validate the information and confirm the identity of the user and inform the External-Entity of the result. Id. at 3:21–26.

This process is described in Claim 1 of the patent, which is representative:

> A method for authenticating a user during an electronic transaction between the user and an external-entity, the method comprising:
>
> receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity;
>
> generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;
>
> providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction;
>
> receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity

> based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction; and
>
> authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid.

The dependent claims build on this basic framework. Independent Claim 25 is an apparatus claim version of Claim 1. Claim 25 requires that two computers perform the functions of the Central-Entity—one to generate a dynamic code and a second to validate it. Independent Claim 48 is another method claim very similar to Claim 1. It requires an alphanumeric dynamic code. Independent Claim 52 is an apparatus claim version of Claim 48 and again uses two computers to perform the functions of the Central-Entity. All independent and dependent claims of the patent require a Central-Entity, a user, and an External-Entity. See '432 patent, Claims 1–55. All claims also require the use of a dynamic code. Id.

II. LEGAL PRINCIPLES

Section 101 of the Patent Act defines the subject matter eligible for patent protection. It provides:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent

> therefor, subject to the conditions and requirements of this title.

35 U.S.C. § 101. The Supreme Court has long recognized an implicit exception to this provision and held that three categories of subject matter are not eligible for patent protection: laws of nature, natural phenomena, and abstract ideas. Alice Corp. Pty. v. CLS Bank Int'l, 134 S.Ct. 2347, 2354 (2014). In Mayo Collaborative Services v. Prometheus Laboratories, Inc., 132 S.Ct. 1289 (2012), the Supreme Court set forth a two-part framework for distinguishing patents that claim one of these patent-ineligible concepts from those that claim patent-eligible applications of these concepts. Alice, 134 S.Ct. at 2355. In the first step, a court determines whether the claims at issue are directed to a patent-ineligible concept. Id. (citing Mayo, 132 S.Ct. at 1286-97). If so, in the second step, a court must consider "what else" is in the claims that may justify patent protection. Id. (quoting Mayo, 132 S.Ct. at 1297). A court must "consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application." Id. (internal quotations omitted) (quoting Mayo, 132 S.Ct. at 1298, 1297). This second step is a search for an "inventive concept" that ensures that the patent claims amount to "significantly more" than claims upon an ineligible concept. Id. (quoting Mayo, 132 S.Ct. at 1294).

Patentability under section 101 is an issue of law that may be resolved on a Rule 12(b)(6) motion to dismiss. Content Extraction & Transmission LLC v. Wells Fargo Bank. Nat. Ass'n, 776 F.3d 1343, 1349

(Fed. Cir. 2014). Claim construction is not necessary to dismiss patent claims at the pleading stage if the construction advocated by the patent holder would not make the claims eligible for patent protection. Id. In determining patent eligibility a court does not need to address each individual claim if the court can identify a representative claim and "all claims are substantially similar and linked to the same abstract idea." Id. at 1348 (internal quotation omitted).

III. ANALYSIS

A. MAYO/ALICE STEP ONE

In Alice, the leading Supreme Court case holding that patent claims were invalid because directed to an abstract idea, the Supreme Court declined "to delimit the precise contours of the 'abstract ideas' category." See 132 S.Ct. at 2357. Recognizing that "precision has been elusive in defining an all-purpose boundary between the abstract and the concrete," Internet Patents Corp. v. Active Network. Inc., 790 F.3d 1343, 1345 (Fed. Cir. 2015), the Federal Circuit has looked to "some important principles" laid down by the Supreme Court in recent cases to decide what is an abstract idea. Content Extraction, 776 F.3d at 1256. For instance, the Supreme Court has held that fundamental economic and longstanding commercial practices are "methods of organizing human activity" that are "within the realm of 'abstract ideas'" as the term is used in section 101 analysis. Alice, 134 S.Ct. at 2356–57. The Supreme Court and Federal Circuit have also compared the claims under review to those found to be directed to an abstract idea in prior cases. Id. at 2355–57 (comparing the claims at issue to those in Bilski v. Kappos, 561 U.S. 593 (2010)); Enfish, LLC v.

Microsoft Corp., No. 2015-1244, 2016 WL 2756255, at *4 (Fed. Cir. May 12, 2016) (identifying this comparative approach).

There have been somewhat contradictory points of emphasis in the opinions of the Supreme Court and Federal Circuit that address what constitutes an abstract idea. In the few cases that the Supreme Court has chosen to take it has consistently found that the patent claims were directed to an abstract idea. See, e.g., Alice, 134 S.Ct. at 2356 (finding the concept of intermediate settlement to be patent ineligible); Bilski, 561 U.S. at 611 (same for the "fundamental economic practice" of hedging). By contrast, the Federal Circuit has cautioned that the "first step of the [Mayo/Alice] inquiry is a meaningful one,... a substantial class of claims are not directed to a patent-ineligible concept." Enfish, 2016 WL 2756255, at *4. Additionally, the Federal Circuit—with support from language in Alice—has warned that describing claims at "a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 shallow the rule." Id. at *6; see also Alice, 134 S.Ct. at 2354 ("[W]e tread carefully in construing this exclusionary principle [concerning laws of nature, natural phenomena, and abstract ideas] lest it shallow all of patent law.").

Critically for the present case, the Federal Circuit has added a new inquiry to step one of the Mayo/Alice analysis when the claims involve computer-related technology. The goal of this inquiry is to distinguish between claims that "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the

Internet" and those that are "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." DDR Holdings, LLC v. Hotels.com. L.P., 773 F.3d 1245, 1257 (Fed. Cir. 2014). The patent claims in Alice were of the first variety: the claims at issue related to a computerized scheme for mitigating settlement risk by means of a third party, a concept the Supreme Court found to be a standard business practice predating the use of computers. See Alice, 134 S.Ct. at 2352, 2356. Although the Supreme Court considered the significance of computerization in performing the second step of the Mayo/Alice analysis, computerization did not factor into the Supreme Court's analysis of the first step. Compare id. at 2355–57 and id. at 2357–60. However, the Federal Circuit has begun to ask "whether the claims are directed to an improvement to computer technology versus being directed to an abstract idea, even at the first step of the Alice analysis." Enfish, 2016 WL 2756255, at *4. Claims that are directed to an improvement to computer technology are not directed to an abstract idea. Id. at *8.

All of the claims in the '432 patent require the use of a computer. Claim 1 of the patent, which is representative, claims a "method for authenticating a user during an electronic transaction." However, despite the electronic setting and purportedly Internet specific problem addressed, the patent claims are directed to a common method for solving an old problem. The claims are directed to the abstract idea of using a third party and a random, time-sensitive code to confirm the identity of a participant to a transaction. This formulation is admittedly verbose. It is verbose because the patent claims combine two abstract ideas:

the use of a third party intermediary to confirm the identity of a participant to a transaction and the use of a temporary code to confirm the identity of a participant to a transaction. It is an obvious combination, and nothing about the combination removes the patent claims from the realm of the abstract.

Nothing about the concept behind the patent claims depends upon their implementation by computers. As USAA points out, the concept could easily be performed either by hand or, more simply, with technologies much older than computers. See USAA's Mem. at 17–18. To adapt USAA's example, let's say that a company (the user, in the terms of the patent) wants to buy a new chair. A local retailer (the External-Entity) will sell goods on credit to anyone who has an account at a local bank (the Central-Entity). By previous arrangement, when the company needs something from the retailer an employee will go to the manager of the bank. The manager will, using a set of dice containing both letters and numbers, generate a random code. The manager writes down this code as well as an expiration time for the code and gives it to the employee. The employee then goes to the retailer. The retailer calls the bank manager and confirms that the code is correct and still valid. The code confirmed, the retailer knows that the individual is an employee of a company that has an account at the bank. The retailer gives the employee a chair.

If this seems a rather involved way to purchase a chair, imagine instead that an intelligence service has a source within a foreign country. Periodically the source (the External-Entity) conveys a packet of

information to a courier (the user) sent by the intelligence service. Although the same courier is never used twice, it is important that the source confirm the identity of the courier. By previous arrangement, whenever a courier goes to pick up the packet the courier first visits the source's handler (the Central-Entity), who works at an embassy in the foreign country. The handler gives the courier a time sensitive code. The courier then goes to the source and tells the source the code. The source relays the code back to the handler who confirms its validity and thus the identity of the courier. The packet is then handed over.

A comparison with the claims at issue in Alice is instructive. The claims in Alice related to a "computerized scheme for mitigating 'settlement risk'—i.e., the risk that only one party to an agreed-upon financial exchange will satisfy its obligation." 134 S.Ct. at 2352. The patent claims were drawn to an old solution to this problem, "intermediated settlement, i.e., the use of a third party to mitigate settlement risk." Id. at 2356. Like the claims in this case, intermediate settlement could and had been performed without computers. The Supreme Court in Alice had no trouble concluding that intermediated settlement was longstanding "method of organizing human activity." Id. The fact that the patent claims used a computer to perform part of this method was of no consequence.

The claims in the '432 patent are not like those considered in the recent Federal Circuit cases that have held that the patent claims under review were not directed to an abstract idea because they were directed to an improvement in computer technology. In DDR Holdings the patent claims were directed to "systems

and methods of generating a composite webpage that combines certain visual elements of a 'host' website with content of a third party merchant." 773 F.3d at 1248. The purpose of this system is to prevent the loss of web traffic that occurs when visitors to a "host" website click an advertisement on the website. Id. In the patented system, when visitors click an advertisement on a "host" webpage, rather than being directed away from the "host" website and to the advertiser's website, the visitors are directed to a hybrid website that maintains the "look and feel" of the "host" website. Id. at 1248–49. It is an Internet-based solution to an Internet-specific problem. Id. at 1257. In Enfish, the patent claims described "an innovative logical model for a computer database" that used a single "self-referential" table to store data. 2016 WL 2756255, at *1. The Federal Circuit held that the patent claims were "directed to a specific improvement to the way computers operate." Id. at *5.

Plaintiffs argue that the patent claims are directed to a "problem unique to computer-network authentication" and could only be implemented by a computer system. Pls.' Opp'n to USAA's Mot. to Dismiss ("Pls.' Opp'n"), ECF No. 101 at 13–14. Certainly it is true that the problem of authenticating parties to a transaction has been magnified by computer and network technology. Through computer networks many individuals may conduct business over long distances in an instance. However, just because a problem has been magnified by computer and network technology does not make the problem unique to this environment. And just as computers magnify the scale of traditional problems such as authentication, they may also make it easier to perform traditional solutions

to these traditional problems. It is true, as Plaintiffs argue, that there are advantages to performing the claimed method on computers. See Pls.' Opp'n at 14-19. However, these advantages do not transform the method into one directed to an improvement of computer technology. Again, a comparison with Alice, the leading Supreme Court case on this issue, is instructive. The risk that one party to a transaction will not follow through on its obligation is undoubtedly magnified for electronic transactions, and there are advantages to performing intermediated settlement using computer technology. This was not enough to save the claims in Alice.

The Federal Circuit itself has emphasized in a recent decision that limiting claims to a particular environment does not necessarily make the claims any less abstract. See In re TLI Commc'ns LLC Patent Litig., No. 2015-1372, 2016 WL 2865693, at *5 (Fed. Cir. May 17, 2016). In TLI Communications, the Federal Circuit considered claims that described a method for recording images with a phone, storing those images as digital images, transmitting the images and classification information collected by the phone to a server, and then sorting the images based on the classification information. See id. at *2 (discussing a representative claim). The Federal Circuit held that the claims were "simply directed to the abstract idea of classifying and storing digital images in an organized manner." Id. at *5. Of course, digital camera technology, in allowing pictures to be taken and developed quickly, magnifies the problem of image classification. Fortunately computers and phones also make it easier to classify and sort images.

B. MAYO/ALICE STEP TWO

Having determined that the claims are directed to an abstract idea, in the second step of the Mayo/Alice analysis the Court must consider whether the elements of the claims both individually and as an ordered combination transform the nature of the claims into a patent-eligible application. This is a search for an "inventive concept." In Alice, the Supreme Court reiterated that "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." 134 S.Ct. at 2358. Were that the case, "any application could claim any principle of the physical or social sciences by reciting a computer system configured to implement the relevant concept. Id. at 2359.

The representative method claim in this case describes the following steps: (1) "receiving" electronically a request for a dynamic code for the user; (2) "generating" by the Central-Entity a dynamic code; (3) "providing" the generated dynamic code to the user; (4) "receiving" electronically by the Central-Entity a request for authenticating the user from a computer associated with the External-Entity; and (5) "authenticating" by the Central-Entity the user and providing the result to the External-Entity. '432 patent, Claim 1.

Taken individually, each of these claim elements describes conventional computer functions. The claim elements describe sending data electronically, generating a random code, and comparing two pieces of data to see if they are the same. As in Alice, "each step does no more than require a generic computer to perform generic computer functions." 134 S.Ct. at 2360.

Considered as an ordered combination, the claim elements do not add anything inventive to the abstract concept underlying them. They simply instruct a generic computer or computers to verify the identity of a participant to a transaction using a randomly generated code. They do not "purport to improve the functioning of the computer itself." Id. "Nor do they effect an improvement in any other technology or technological field." Id. They have generic computers perform an old method of authentication. This is not enough to transform a patent-ineligible abstract idea into a patent-eligible invention. See id. at 2360.

Put simply, there is nothing inventive about Plaintiffs' patent claims. To allow Plaintiffs to patent a generic computer implementation of an abstract idea would allow Plaintiffs to monopolize the idea itself and inhibit further discovery and invention. See id. at 2354, 2359.

C. THE NEED FOR CLAIM CONSTRUCTION AND THE APPARATUS CLAIMS

Finally, the Court notes that while Plaintiffs recite the need for claim construction, they never identify how claim construction might change the meaning of the claims such that they would be eligible for patent protection. Additionally, although Plaintiffs fault USAA for focusing its analysis on Claim 1 of the '432 patent, they fail to specify how consideration of the other claims would add to the analysis. This is not to say that Plaintiffs have the burden to prove the validity of their patent. The point is simply that Plaintiffs' arguments on these points are empty. As described above, all of the claims are substantially similar to Claim 1. Independent method Claim 48 adds the

limitation of an alphanumeric dynamic code. The two apparatus claims, Claims 25 and 51, simply use two computers to perform the functions of the Central-Entity. None of these additional limitations change the substance of the claims. See Alice, 134 S.Ct. at 2360 ("Put another way, the system claims are no different from the method claims in substance. The method claims recite the abstract idea implemented on a generic computer; the system claims recite a handful of generic computer components configured to implement the same idea."). Similarly, construction of the claims would not affect the Court's analysis of whether the claims are directed to an abstract idea. No matter what construction the Court adopts the substance of the claims is the same.

IV. CONCLUSION

For the above reasons, the Court holds that the claims of the '432 patent at issue are invalid because they are directed to an abstract idea and thus ineligible for patent protection under 35 U.S.C. § 101. Because the allegedly infringed patent claims are invalid, Plaintiffs fail to state a claim for relief. Accordingly, the Court **GRANTS** the Motion to Dismiss, ECF No. 86, and **DISMISSES** Plaintiffs' Second Amended Complaint **WITH PREJUDICE**, ECF No. 70. The Court also **DISMISSES AS MOOT** USAA's Counterclaims. ECF No. 88.

The Clerk is **DIRECTED** to forward a copy of this Order to all Counsel of Record.

IT IS SO ORDERED.

s/_____
UNITED STATES DISTRICT JUDGE

Norfolk, VA
July 5, 2016

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CIVIL NO. 2:15cv478

[Filed July 5, 2016]

NADER ASGHARI-KAMRANI and KAMRAN ASGHARI-KAMRANI	)
Plaintiffs,	)
v.	)
UNITED SERVICES AUTOMOBILE ASSOCIATION	)
Defendant.	)

JUDGMENT IN A CIVIL CASE

Decision by Court: This action came on for decision before the Court. The issues have been decided and a decision has been rendered.

IT IS ORDERED,ADJUDGED and DECREED the Court holds that the claims of the '432 patent at issue are invalid because they are directed to an abstract idea and thus ineligible for patent protection under 35 U.S.C. § 101. Because the allegedly infringed patent claims are invalid. Plaintiffs fail to state a claim for relief. Accordingly, the Court **GRANTS** the Motion to Dismiss, ECF No. 86, and **DISMISSES** Plaintiffs' Second Amended Complaint **WITH PREJUDICE**,

ECF No. 70. The Court also **DISMISSES AS MOOT** USAA's Counterclaims. ECF No. 88.

July 5, 2016
Date

FERNANDO GALINDO, CLERK

By: /s/
Lara Dabbene, Deputy Clerk

APPENDIX C

NOTE: This disposition is nonprecedential.

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

2016-2415, 2017-2101, 2017-2191

[Filed November 14, 2018]

KAMRAN ASGHARI-KAMRANI, NADER ASGHARI-KAMRANI, *Plaintiffs-Appellants*

v.

UNITED SERVICES AUTOMOBILE ASSOCIATION, *Defendant-Cross-Appellant*

Appeals from the United States District Court for the Eastern District of Virginia in No. 2:15-cv-00478-RGD-LRL, Senior Judge Robert G. Doumar.

ON PETITION FOR REHEARING EN BANC

Before PROST, *Chief Judge*, NEWMAN, LOURIE, DYK, MOORE, O'MALLEY, REYNA, WALLACH, TARANTO, CHEN, HUGHES, and STOLL, *Circuit Judges*.

PER CURIAM.

O R D E R

Appellants Kamran Asghari-Kamrani and Nader Asghari-Kamrani filed a petition for rehearing en banc. The petition was first referred as a petition for rehearing to the panel that heard the appeal, and thereafter the petition for rehearing en banc was referred to the circuit judges who are in regular active service.

Upon consideration thereof,

IT IS ORDERED THAT:

The petition for panel rehearing is denied.

The petition for rehearing en banc is denied.

The mandate of the court will issue on November 21, 2018.

FOR THE COURT

November 14, 2018
Date

/s/ Peter R. Marksteiner
Peter R. Marksteiner
Clerk of Court

APPENDIX D

US Constitution, art. I, § 8, cl. 8 and 15.

The Congress shall have power to lay and collect taxes, duties, imposts and excises, to pay the debts and provide for the common defense and general welfare of the United States; but all duties, imposts and excises shall be uniform throughout the United States;

***

To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries; . . .

To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.

35 U.S.C. § 101. Inventions patentable

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

APPENDIX D

Patent No.: US 8,266,432 B2

See Fold-Out Exhibit

US008266432B2

(12) **United States Patent**
Asghari-Kamrani et al.

(10) **Patent No.: US 8,266,432 B2**
(45) **Date of Patent: *Sep. 11, 2012**

(54) **CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD**

(76) Inventors: **Nader Asghari-Kamrani**, Centreville, VA (US); **Kamran Asghari-Kamrani**, Centreville, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/210,926**

(22) Filed: **Sep. 15, 2008**

(65) **Prior Publication Data**

US 2009/0013182 A1 Jan. 8, 2009

Related U.S. Application Data

(63) Continuation of application No. 11/239,046, filed on Sep. 30, 2005, now Pat. No. 7,444,676, which is a continuation of application No. 09/940,635, filed on Aug. 29, 2001, now Pat. No. 7,356,837.

(60) Provisional application No. 60/615,603, filed on Oct. 5, 2004.

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06Q 20/00 (2012.01)

(52) **U.S. Cl.** **713/168**; 713/184; 705/67; 705/74; 705/78

(58) **Field of Classification Search** 726/21, 726/2–5, 212, 8, 18, 27, 28; 713/155, 168, 713/170, 182–186; 705/35, 39, 44, 50, 64, 705/67, 72, 76, 78

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,747,050	A	5/1988	Brachtl et al.	
4,965,568	A	10/1990	Atalla et al.	
5,535,276	A *	7/1996	Ganesan	713/155
5,732,137	A *	3/1998	Aziz	713/155
5,883,810	A *	3/1999	Franklin et al.	700/232
6,067,621	A *	5/2000	Yu et al.	713/172
6,236,981	B1 *	5/2001	Hill	705/67
6,338,140	B1 *	1/2002	Owens et al.	713/168

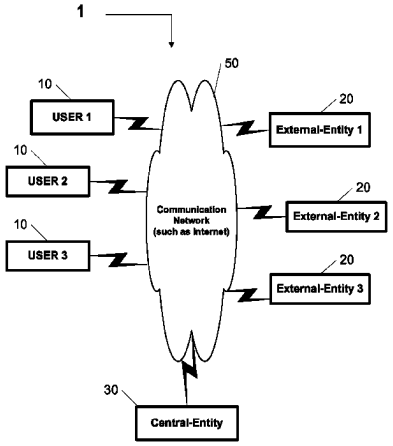
(Continued)

Primary Examiner — Gilberto Barron, Jr.
Assistant Examiner — Abdulhakim Nobahar
(74) *Attorney, Agent, or Firm* — Michael P. Fortkort, Esq.; Michael P Fortkort PC

(57) **ABSTRACT**

A method and system is provided by a Central-Entity, for identification and authorization of users over a communication network such as Internet. Central-Entity centralizes users personal and financial information in a secure environment in order to prevent the distribution of user's information in e-commerce. This information is then used to create digital identity for the users. The digital identity of each user is dynamic, non predictable and time dependable, because it is a combination of user name and a dynamic, non predictable and time dependable secure code that will be provided to the user for his identification. The user will provide his digital identity to an External-Entity such as merchant or service provider. The External-Entity is dependent on Central-Entity to identify the user based on the digital identity given by the user. The External-Entity forwards user's digital identity to the Central-Entity for identification and authentication of the user and the transaction. The identification and authentication system provided by the Central-Entity, determines whether the user is an authorized user by checking whether the digital identity provided by the user to the External-Entity, corresponds to the digital identity being held for the user by the authentication system. If they correspond, then the authentication system identifies the user as an authorized user, and sends an approval identification and authorization message to the External-Entity, otherwise the authentication system will not identify the user as an authorized user and sends a denial identification and authorization message to the External-Entity.

55 Claims, 5 Drawing Sheets



U.S. PATENT DOCUMENTS

6,529,885	B1 *	3/2003	Johnson	705/64
6,715,082	B1 *	3/2004	Chang et al.	726/8
7,150,038	B1 *	12/2006	Samar	726/8
7,353,541	B1 *	4/2008	Ishibashi et al.	726/26
7,546,274	B2 *	6/2009	Ingram et al.	705/43
2002/0040346	A1 *	4/2002	Kwan	705/51
2002/0046189	A1 *	4/2002	Morita et al.	705/67
2002/0069174	A1 *	6/2002	Fox et al.	705/52
2002/0133412	A1 *	9/2002	Oliver et al.	705/26
2002/0184143	A1 *	12/2002	Khater	705/39
2002/0188481	A1 *	12/2002	Berg et al.	705/4
2004/0030752	A1 *	2/2004	Selgas et al.	709/206
2005/0222963	A1 *	10/2005	Johnson	705/67
2007/0073621	A1 *	3/2007	Dulin et al.	705/50
2008/0016003	A1 *	1/2008	Hutchison et al.	705/67
2010/0100724	A1 *	4/2010	Kaliski, Jr.	713/155

* cited by examiner

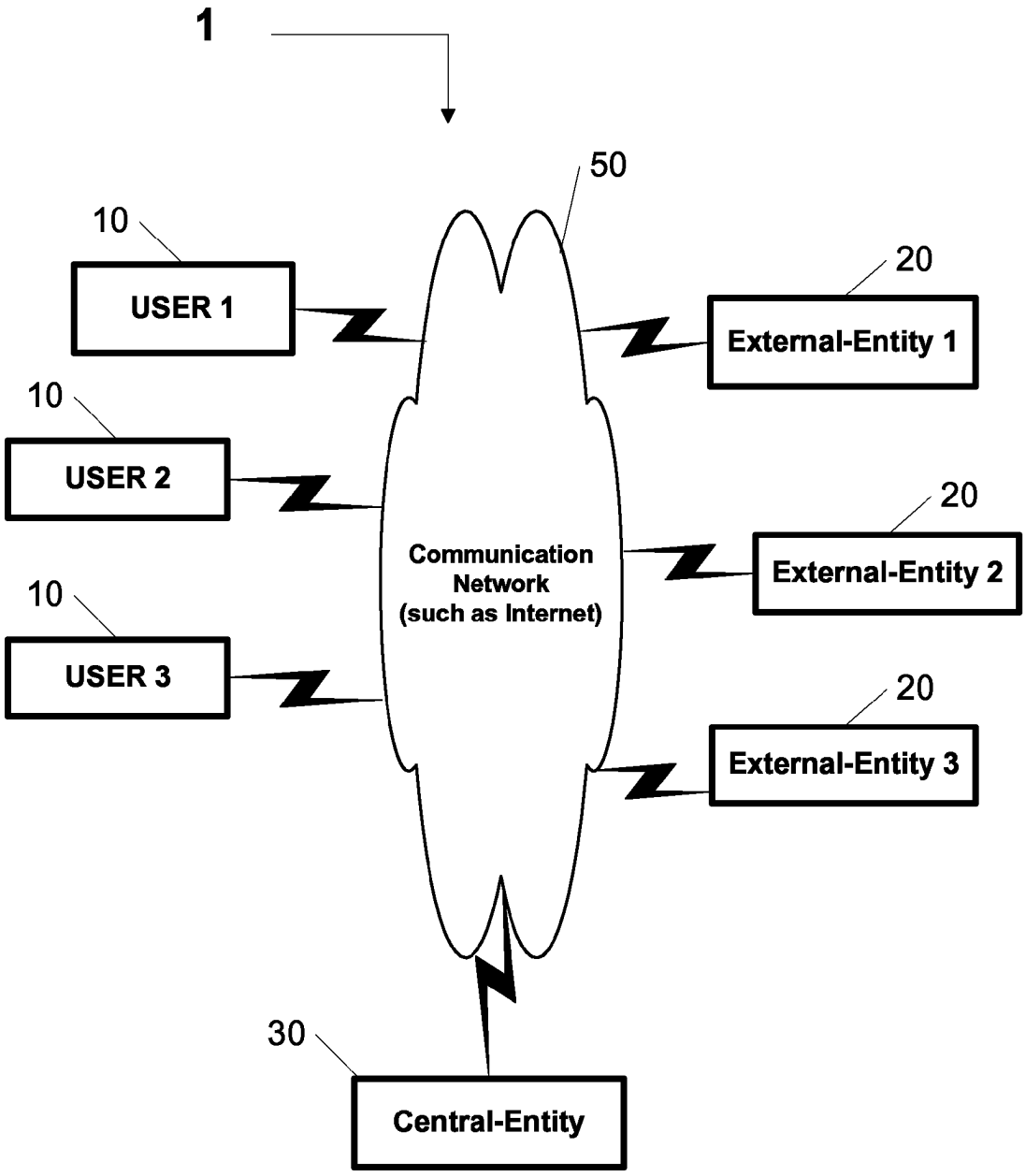
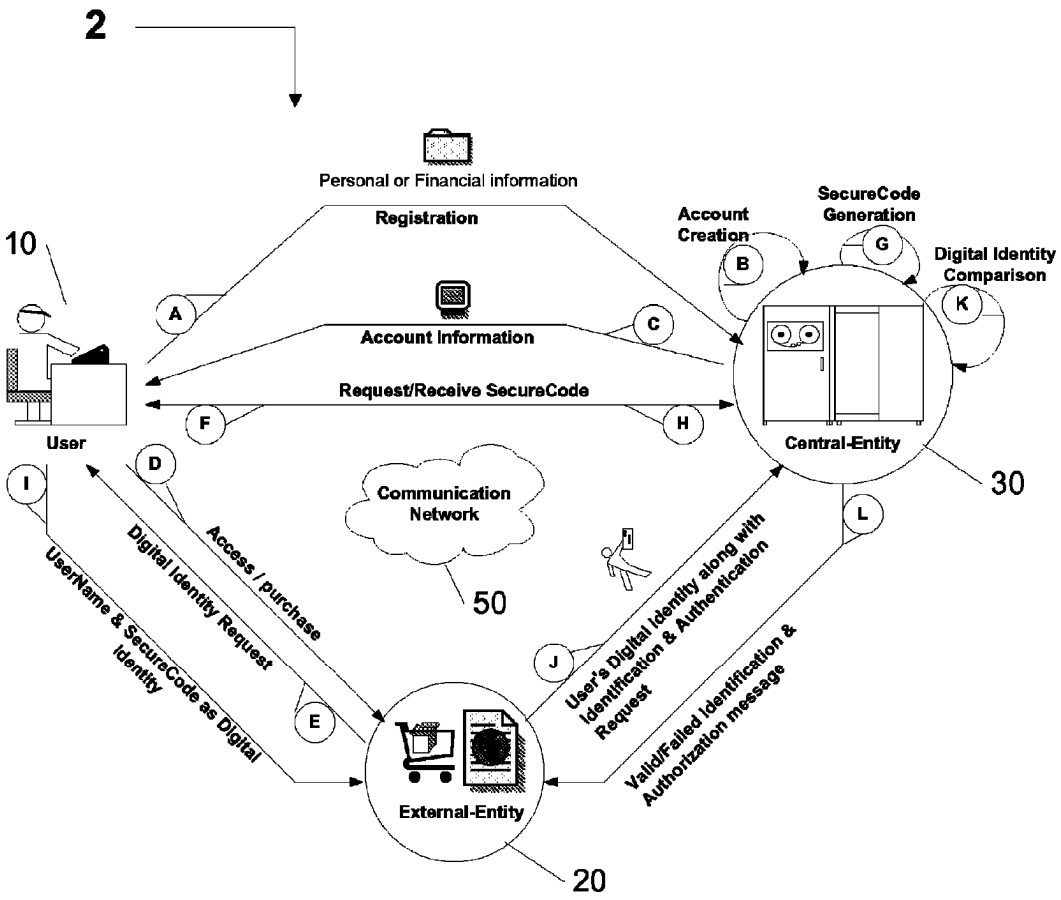

1
50
10
USER 1
10
USER 2
10
USER 3
Communication Network (such as Internet)
20
External-Entity 1
20
External-Entity 2
20
External-Entity 3
30
Central-Entity

Figure 1



Registration Phase Steps: A B C

Transaction Phase Steps: D E F G H I

Identification & Authorization Phase Steps: J K L

Figure 2

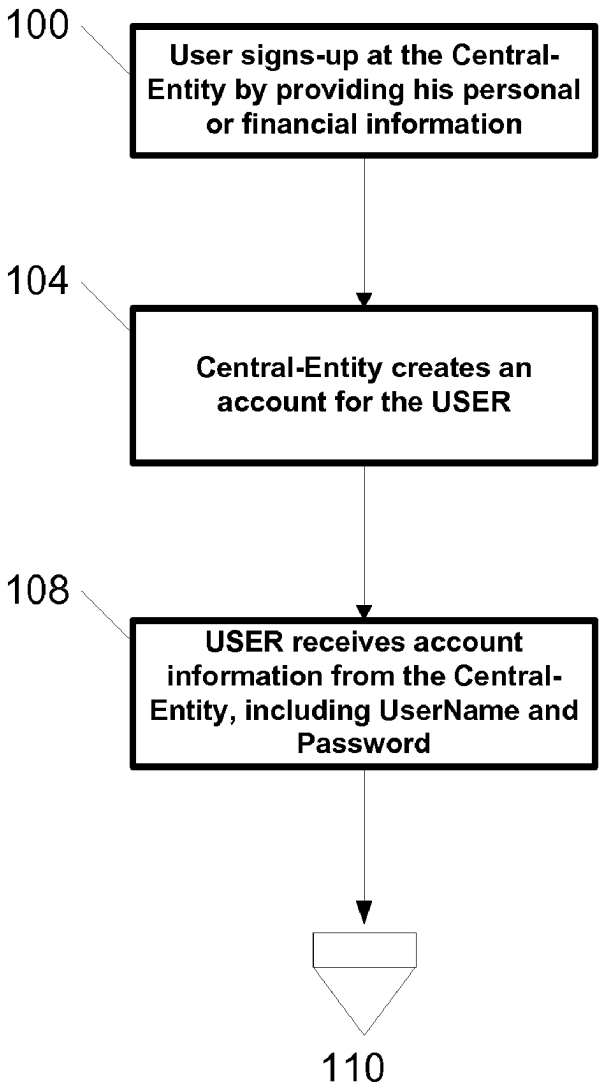

100
User signs-up at the Central-Entity by providing his personal or financial information
104
Central-Entity creates an account for the USER
108
USER receives account information from the Central-Entity, including UserName and Password
110

Figure 3

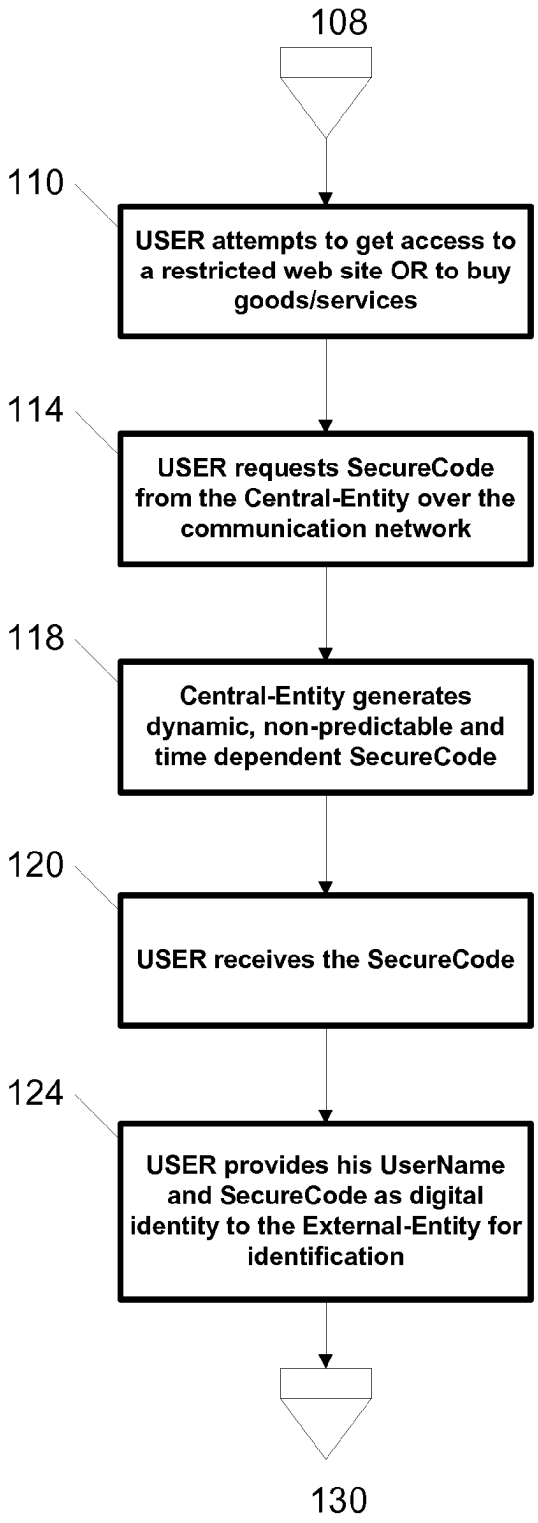

108
110
USER attempts to get access to a restricted web site OR to buy goods/services
114
USER requests SecureCode from the Central-Entity over the communication network
118
Central-Entity generates dynamic, non-predictable and time dependent SecureCode
120
USER receives the SecureCode
124
USER provides his UserName and SecureCode as digital identity to the External-Entity for identification
130

Figure 4

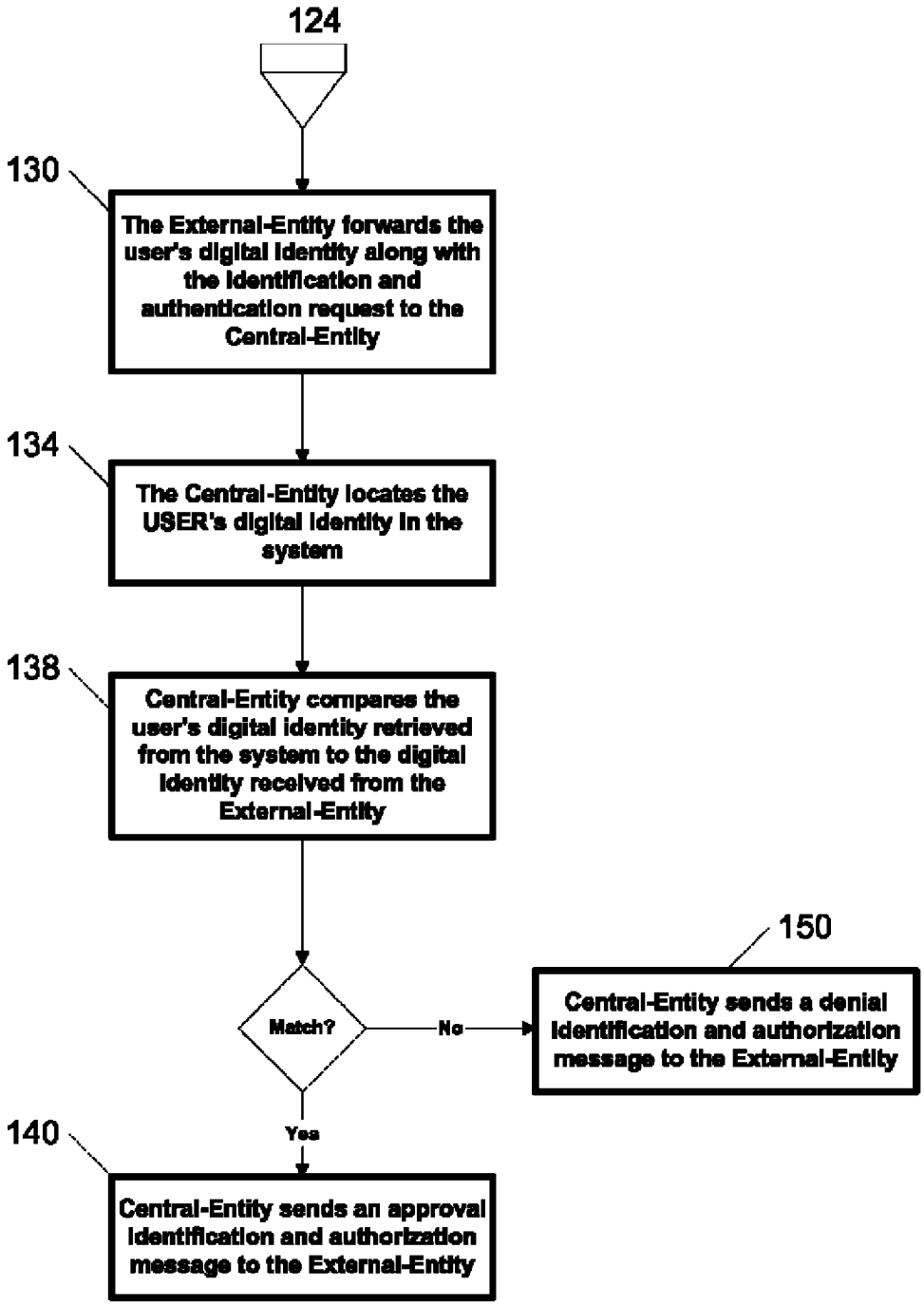

124
130
The External-Entity forwards the user's digital identity along with the identification and authentication request to the Central-Entity
134
The Central-Entity locates the USER's digital identity in the system
138
Central-Entity compares the user's digital identity retrieved from the system to the digital identity received from the External-Entity
Match?
No
150
Central-Entity sends a denial identification and authorization message to the External-Entity
Yes
140
Central-Entity sends an approval identification and authorization message to the External-Entity

Figure 5

CENTRALIZED IDENTIFICATION AND AUTHENTICATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application is a Continuation of application Ser. No. 11/239,046, filed Sep. 30, 2005 now U.S. Pat. No. 7,444,676, with a priority of a U.S. provisional application 60/615,603, filed Oct. 5, 2004, with the same inventors and assignee. This application is also a Continuation of another U.S. application Ser. No. 09/940,635, filed Aug. 29, 2001, and patented as U.S. Pat. No. 7,356,837, on Apr. 8, 2008, titled "Centralized identification and authentication system and method", with the same inventors and assignee. Please note that the current application has the same exact specification and Figures as those submitted with the original application Ser. No. 09/940,635, filed Aug. 29, 2001.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a centralized identification and authentication system and method for identifying an individual over a communication network such as Internet, to increase security in e-commerce. More particularly a method and system for generation of a dynamic, non-predictable and time dependent SecureCode for the purpose of positively identifying an individual.

2. Description of the Related Art

The increasing use of the Internet and the increase of businesses utilizing e-commerce have lead to a dramatic increase in customers releasing confidential personal and financial information, in the form of social security numbers, names, addresses, credit card numbers and bank account numbers, to identify themselves. This will allow them to get access to the restricted web sites or electronically purchase desired goods or services. Unfortunately this type of identification is not only unsafe but also it is not a foot proof that the user is really the person he says he is. The effect of these increases is reflected in the related art.

U.S. Pat. No. 5,732,137 issued to Aziz outlines a system and method for providing remote user authentication in a public computer network such as the Internet. More specifically, the system and method provides for remote authentication using a one-time password scheme having a secure out-of-band channel for initial password delivery.

U.S. Pat. No. 5,815,665 issued to Teper et al. outlines the use of a system and method for enabling consumers to anonymously, securely and conveniently purchase on-line services from multiple service providers over a distributed network, such as the Internet. Specifically, a trusted third-party broker provides billing and security services for registered service providers via an online brokering service, eliminating the need for the service providers to provide these services.

U.S. Pat. No. 5,991,408 issued to Pearson, et al. outlines a system and method for using a biometric element to create a secure identification and verification system, and more specifically to an apparatus and a method for creating a hard problem which has a representation of a biometric element as its solution.

Although each of the previous patents outline a valuable system and method, what is really needed is a system and method that offers digital identity to the users and allows them to participate in e-commerce without worrying about the privacy and security. In addition to offering security and privacy to the users, the new system has to be simple for businesses to adopt and also doesn't require the financial

institutions to change their existing systems. Such a secure, flexible and scalable system and method would be of great value to the businesses that would like to participate in today's electronic commerce.

None of the above inventions and patents, taken either singularly or in combination, is seen to describe the instant invention as claimed. Thus a centralized identification and authentication system and method solving the aforementioned problems is desired.

For convenience, the term "user" is used throughout to represent both a typical person consuming goods and services as well as a business consuming goods and services.

As used herein, a "Central-Entity" is any party that has user's personal and/or financial information, UserName, Password and generates dynamic, non-predictable and time dependable SecureCode for the user. Examples of Central-Entity are: banks, credit card issuing companies or any intermediary service companies.

As also used herein, an "External-Entity" is any party offering goods or services that users utilize by directly providing their UserName and SecureCode as digital identity. Such entity could be a merchant, service provider or an online site. An "External-Entity" could also be an entity that receives the user's digital identity indirectly from the user through another External-Entity, in order to authenticate the user, such entity could be a bank or a credit card issuing company.

The term "UserName" is used herein to denote any alphanumeric name, id, login name or other identification phrase, which may be used by the "Central-Entity" to identify the user.

The term "Password" is used herein to denote any alphanumeric password, secret code, PIN, prose phrase or other code, which may be stored in the system to authenticate the user by the "Central-Entity".

The term "SecureCode" is used herein to denote any dynamic, non-predictable and time dependent alphanumeric code, secret code, PIN or other code, which may be broadcast to the user over a communication network, and may be used as part of a digital identity to identify a user as an authorized user.

The term "digital identity" is used herein to denote a combination of user's "SecureCode" and user's information such as "UserName", which may result in a dynamic, non-predictable and time dependable digital identity that could be used to identify a user as an authorized user.

The term "financial information" is used herein to denote any credit card and banking account information such as debit cards, savings accounts and checking accounts.

SUMMARY OF THE INVENTION

The invention relates to a system and method provided by a Central-Entity for centralized identification and authentication of users and their transactions to increase security in e-commerce. The system includes:

- A Central-Entity: This entity centralizes users personal and financial information in a secure environment in order to prevent the distribution of user's information in e-commerce. This information is then used to create digital identity for the users. The users may use their digital identity to identify themselves instead of providing their personal and financial information to the External-Entities;
- A plurality of users: A user represents both a typical person consuming goods and services as well as a business consuming goods and services, who needs to be identified in order to make online purchases or to get access to

the restricted web sites. The user registers at the Central-Entity to receive his digital identity, which is then provided to the External-Entity for identification;

A plurality of External-Entities: An External-Entity is any party offering goods or services in e-commerce and needs to authenticate the users based on digital identity.

The user signs-up at the Central-Entity by providing his personal or financial information. The Central-Entity creates a new account with user's personal or financial information and issues a unique UserName and Password to the user. The user provides his Username and Password to the Central-Entity for identification and authentication purposes when accessing the services provided by the Central-Entity. The Central-Entity also generates dynamic, non-predictable and time dependent SecureCode for the user per user's request and issues the SecureCode to the user. The Central-Entity maintains a copy of the SecureCode for identification and authentication of the user's digital identity. The user presents his UserName and SecureCode as digital identity to the External-Entity for identification. When an External-Entity receives the user's digital identity (UserName and SecureCode), the External-Entity will forward this information to the Central-Entity to identify and authenticate the user. The Central-Entity will validate the information and sends an approval or denial response back to the External-Entity.

There are also communications networks for the user, the Central-Entity and the External-Entity to give and receive information between each other.

This invention also relates to a system and method provided by a Central-Entity for centralized identification and authentication of users to allow them access to restricted web sites using their digital identity, preferably without revealing confidential personal or financial information.

This invention further relates to a system and method provided by a Central-Entity for centralized identification and authentication of users to allow them to purchase goods and services from an External-Entity using their digital identity, preferably without revealing confidential personal or financial information.

Accordingly, it is a principal object of the invention to offer digital identity to the users for identification in e-commerce.

It is another object of the invention to centralize user's personal and financial information in a secure environment.

It is another object of the invention to prevent the user from distributing their personal and financial information.

It is a further object of the invention to keep merchants, service providers, Internet sites and financial institutions satisfied by positively identifying and authenticating the users.

It is another object of the invention to reduce fraud and increase security for e-commerce.

It is another object of the invention to allow businesses to control visitor's access to their web sites.

It is another object of the invention to protect the customer from getting bills for goods and services that were not ordered.

It is another object of the invention to increase customers' trust and reduce customers' fear for e-commerce.

It is another object to decrease damages to the customers, merchants and financial institutions.

It is an object of the invention to provide improved elements and arrangements thereof for the purposes described which are inexpensive, dependable and fully effective in accomplishing its intended purposes.

These and other objects of the present invention will become readily apparent upon further review of the following specification and drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a high-level overview of a centralized identification and authentication system and method according to the present invention.

FIG. **2** is a detailed overview of a centralized identification and authentication system and method according to the present invention.

FIG. **3** is a block diagram of the registration of a customer utilizing a centralized identification and authentication system and method according to the present invention.

FIG. **4** is a block diagram of the transaction of a customer utilizing a centralized identification and authentication system and method according to the present invention.

FIG. **5** is a block diagram of a Central-Entity authorizing a user utilizing a centralized identification and authentication system and method according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Detailed descriptions of the preferred embodiment are provided herein. It is to be understood, however, that the present invention may be embodied in various forms. Therefore, specific details disclosed herein are not to be interpreted as limiting, but rather as a basis for the claims and as a representative basis for teaching one skilled in the art to employ the present invention in virtually any appropriately detailed system, structure or manner.

The invention relates to a system **1** and method **2** to identify and authenticate the users and their transactions to increase security in e-commerce. FIG. **1** illustrates a system to positively identify the users **10** in e-commerce based on digital identity.

The system **1** comprises a plurality of users **10**, a plurality of External-Entities **20** with goods and services that are desired by the users **10** and a Central-Entity **30** providing a unique UserName and Password to the users **10** and generating dynamic, non-predictable and time dependent SecureCode for the users **10** per user's request. There are also communication networks **50** for the user **10**, the Central-Entity **30** and the External-Entity **20** to give and receive information between each other.

It would be desirable to develop a new system **1** and method **2** to centralize user's personal and financial information in a secure environment and to offer digital identity to the users **10** in order to provide privacy, increase security and reduce fraud in e-commerce. Ideally, a secure identification and authentication system **1** would identify legitimate users **10** and unauthorized users **10**. This would increase the user's trust, which leads to more sales and cash flow for the merchants/service providers.

The present invention relates to a system **1** and method **2** to support this ideal identification and authentication system. For identification purpose, a digital identity (a unique UserName and a dynamic, non-predictable and time dependent SecureCode) is used by the user **10** at the time of ordering or at the time of accessing a restricted Internet site. A series of steps describing the overall method are conducted between the users **10**, the Central-Entity **30** and the External-Entity **20** and are outlined in FIG. **3**,**4**,**5**.

There are three distinct phases involved in using the centralized identification and authentication system FIG. **2**, the first of which being the registration phase, which is depicted in FIG. **3**. During the registration phase, the user **10** provides his personal or financial information to the Central-Entity **30**. The user **10** registers at the Central-Entity **30**, **100**, **104** and

receives his account and login information such as UserName and Password **108**. User **10** can access his account at any time by accessing the Central-Entity's system using a communication network **50** and logging into the system.

Next is the transaction phase, where the user **10** attempts to access a restricted web site or attempts to buy services or products **110**, as illustrated in FIG. **4**, through a standard interface provided by the External-Entity **20**, similar to what exists today and selects digital identity as his identification and authorization or payment option. The External-Entity **20** displays the access or purchase authorization form requesting the user **10** to authenticate himself using his UserName and SecureCode as digital identity. The user **10** requests SecureCode from the Central-Entity **30** by accessing his account over the communication network **50**, **114**. The Central-Entity **30** generates dynamic, non-predictable and time dependable SecureCode **118** for the user **10**. The Central-Entity **30** maintains a copy of the SecureCode for identification and authentication of the user **10** and issues the SecureCode to the user **10**. When the user **10** receives the SecureCode **120**, the user **10** provides his UserName and SecureCode as digital identity to the External-Entity **20**, **124**, FIG. **4**.

The third phase is identification and authorization phase. Once the user **10** provides his digital identity to the External-Entity **20**, the External-Entity **20** forwards user's digital identity along with the identification and authentication request to the Central-Entity **30**, **130**, as illustrated in FIG. **5**. When the Central-Entity **30** receives the request containing the user's digital identity, the Central-Entity **30** locates the user's digital identity (UserName and SecureCode) in the system **134** and compares it to the digital identity received from the External-Entity **20** to identify and validate the user **10**, **138**. The Central-Entity **30** generates a reply back to the External-Entity **20** via a communication network **50** as a result of the comparison. If both digital identities match, the Central-Entity **30** will identify the user **10** and will send an approval of the identification and authorization request to the External-Entity **20**, **140**, otherwise will send a denial of the identification and authorization request to the External-Entity **20**, **150**. The External-Entity **20** receives the approval or denial response in a matter of seconds. The External-Entity **20** might also display the identification and authentication response to the user **10**.

To use the digital identity feature, the Central-Entity **30** provides the authorized user **10** the capability to obtain a dynamic, non-predictable and time dependable SecureCode. The user **10** will provide his UserName and SecureCode as digital identity to the External-Entity **20** when this information is required by the External-Entity **20** to identify the user **10**.

The Central-Entity **30** may add other information to the SecureCode before sending it to the user **10**, by algorithmically combining SecureCode with user's information such as UserName. The generated SecureCode will have all the information needed by the Central-Entity **30** to identify the user **10**. In this case the user will only need to provide his SecureCode as digital identity to the External-Entity **20** for identification.

In the preferred embodiment, the user **10** uses the communication network **50** to receive the SecureCode from the Central-Entity **30**. The user **10** submits the SecureCode in response to External-Entity's request **124**. The SecureCode is preferably implemented through the use of an indicator. This indicator has two states: "on" for valid and "off" for invalid. When the user **10** receives the SecureCode, the SecureCode is in "on" or "valid" state. The Central-Entity **30** may improve the level of security by invalidating the SecureCode after it's use. This may increase the level of difficulty for unauthorized user. Two events may cause a valid SecureCode to become invalid:

1. Timer event: This event occurs when the predefined time passes. As mentioned above the SecureCode is time dependent.

2. Validation event: This event occurs when the SecureCode forwarded to the Central-Entity **30** (as part of digital identity) corresponds to the user's SecureCode held in the system. When this happens the Central-Entity **30** will invalidate the SecureCode to prevent future use and sends an approval identification and authorization message to the External-Entity **20**,**140**.

A valid digital identity corresponds to a valid SecureCode. When the SecureCode becomes invalid, the digital identity will also become invalid.

While the invention has been described in connection with a preferred embodiment, it is not intended to limit the scope of the invention to the particular form set forth, but on the contrary, it is intended to cover such alternatives, modifications, and equivalents as may be included within the spirit and scope of the invention as defined by the appended claims.

The invention claimed is:

1. A method for authenticating a user during an electronic transaction between the user and an external-entity, the method comprising:

receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the transaction between the user and the external-entity;

generating by the central-entity during the transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

providing by the computer associated with the central-entity said generated dynamic code to the user during the transaction;

receiving electronically by the central-entity a request for authenticating the user from a computer associated with the external-entity based on a user-specific information and the dynamic code as a digital identity included in the request which said dynamic code was received by the user during the transaction and was provided to the external-entity by the user during the transaction; and

authenticating by the central-entity the user and providing a result of the authenticating to the external-entity during the transaction if the digital identity is valid.

2. A method as recited in claim **1**, further comprising:

combining said generated dynamic code with the user-specific information using a predetermined algorithm to form a combined dynamic code and user specific information;

maintaining the combined dynamic code and user specific information at the central-entity;

comparing the combined dynamic code and user specific information with a received combined dynamic code and user specific information to validate the user.

3. The method of claim **1**, wherein the user specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

4. The method of claim **1**, wherein the transaction corresponds to a financial transaction.

5. The method of claim **1**, wherein the transaction corresponds to a non-financial transaction.

6. The method of claim **1**, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

7. The method of claim 1, wherein said transaction occurs over a communication network, wherein said communication network comprises one or more of the following: a public network, the Internet, a wireless network, a mobile network, a satellite network, and a private network.

8. The method of claim 1, wherein said transaction occurs over a communication network to which is coupled said user, said central-entity, and said external-entity.

9. A method as recited in claim 2, wherein said algorithmically combined dynamic code and user specific information is used to authenticate a user's identity.

10. A method as recited in claim 2, wherein said central-entity is using said algorithmically combined dynamic code and user specific information to authenticate a user's identity.

11. A method as recited in claim 1, wherein said external-entity and said central-entity are the same entity.

12. The method as recited in claim 1, wherein said central-entity invalidates the dynamic code after authenticating the user.

13. The method as recited in claim 1, wherein the central-entity invalidates the dynamic code after a predefined period of time passes from when the dynamic code was generated.

14. The method as recited in claim 1, wherein said central-entity generates the dynamic code with dependence on the user information.

15. The method as recited in claim 14, wherein said user information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

16. The method as recited in claim 1, wherein said user communicates with said central-entity over a communication network.

17. The method as recited in claim 1, wherein said user communicates with said external-entity over a communication network.

18. The method as recited in claim 1, wherein said dynamic code is generated based on a request submitted by said user over a communication network.

19. The method as recited in claim 18, wherein said request is initiated by said user through a standard interface provided to said user.

20. A method as recited in claim 1, wherein said digital identity is invalid if the dynamic code is invalid.

21. A method as recited in claim 1, wherein said digital identity is valid if at least the dynamic code is valid.

22. A method as recited in claim 1, wherein said external-entity authenticates the user upon receiving an affirmation authentication message from the central-entity.

23. A method as recited in claim 1, wherein said external-entity authenticates the user if said central-entity authenticates the user based on the dynamic code.

24. The method of claim 1, wherein the user-specific information includes user-identifying information.

25. An apparatus for authenticating a user during an electronic transaction with an external-entity, the apparatus comprising:

a first central-entity computer adapted to:

generate a dynamic code for the user in response to a request during the electronic transaction, wherein the dynamic code is valid for a predefined time and becomes invalid after being used; and

provide said dynamic code to the user during the electronic transaction;

a second central-entity computer adapted to validate a digital identity in response to an authentication request from the external-entity, which authentication request includes a user-specific information and the dynamic code as the digital identity which dynamic code was received by the user during the electronic transaction and was provided to the external-entity by the user during the electronic transaction, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction.

26. The apparatus as recited in claim 25, wherein said user has a pre-existing relationship with the external-entity.

27. The apparatus as recited in claim 25, wherein said user has no pre-existing relationship with the external-entity.

28. The apparatus as recited in claim 25, wherein said external-entity and said central-entity use a dynamic code that is algorithmically combined with said the user-specific information.

29. The apparatus of claim 25, wherein the transaction corresponds to a financial transaction.

30. The apparatus of claim 25, wherein the transaction corresponds to a non-financial transaction.

31. The apparatus of claim 25, wherein the transaction corresponds to access to restricted web-site or restricted computer/server.

32. The apparatus of claim 25, wherein said transaction occurs over a communication network and wherein said communication network comprises one or more of the following: a public network, the Internet, a wireless network, a mobile network, a satellite network, and a private network.

33. The apparatus of claim 25, wherein said transaction occurs over a communication network to which is coupled said user, said central-entity, and said external-entity.

34. The apparatus as recited in claim 25, wherein said user communicates with said central-entity over a communication network.

35. The apparatus as recited in claim 25, wherein said user communicates with said external-entity over a communication network.

36. The apparatus according to claim 25, wherein said first central-entity computer and said second central-entity computer are the same.

37. The apparatus according to claim 25, wherein said first central-entity computer and said second central-entity computer are different.

38. The apparatus of claim 25, wherein said digital identity is invalid if the dynamic code is invalid.

39. The apparatus of claim 25, wherein said digital identity is valid if at least the dynamic code is valid.

40. The apparatus of claim 25, wherein said external-entity authenticates the user upon receiving an affirmation authentication message from the central-entity.

41. The apparatus of claim 25, wherein said central-entity invalidates the dynamic code after authenticating the user.

42. The apparatus of claim 25, wherein the central-entity invalidates the dynamic code after a predefined period of time passes after the dynamic code was generated.

43. The apparatus of claim 25, wherein said central-entity generates the dynamic code based on said user-specific information.

44. The apparatus of claim 43, wherein said user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, a password, and an identification phrase.

45. The apparatus of claim 25, wherein said external-entity authenticates the user if said central-entity authenticates the user based on the dynamic code.

46. The apparatus of claim 25, wherein said external-entity and central-entity are the same entity.

47. The apparatus of claim 25, wherein the user-specific information includes user-identifying information.

48. A method for authenticating a user during an electronic transaction between the user and an external-entity, the method comprising:

receiving electronically a request for a dynamic code for the user by a computer associated with a central-entity during the electronic transaction between the user and the external-entity;

generating by the central-entity during the electronic transaction a dynamic code for the user in response to the request, wherein the dynamic code is valid for a predefined time and becomes invalid after being used;

providing by a computer associated with the central-entity said generated dynamic code to the user during the transaction;

receiving during the electronic transaction by another computer associated with the central-entity a request from the external-entity for authenticating the user based on a user-specific information and the dynamic code as a digital identity included in the request, which said dynamic code was received by the user during the transaction and was provided by the user to the external-entity during the electronic transaction; and

authenticating by the central-entity the user and providing a result of the authentication of the user to the external-entity during the transaction if the digital identity is valid, wherein said dynamic code is alphanumeric.

49. A method as recited in claim 48, wherein said external-entity and central-entity are the same entity.

50. The method of claim 48, wherein the user-specific information includes user-identifying information.

51. The method of claim 48, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

52. An apparatus for authenticating a user during an electronic transaction with an external-entity, the apparatus comprising:

a first central-entity computer adapted to:

generate a dynamic code for the user in response to a request from the user during the electronic transaction, wherein the dynamic code is valid for a predefined time and becomes invalid after being used; and

provide said dynamic code to the user during the electronic transaction;

a second central-entity computer adapted to validate a user-specific information and the dynamic code as a digital identity included in an authentication request from the external-entity, which said dynamic code was received by the user during the electronic transaction and was provided by the user to the external-entity during the electronic transaction, and to authenticate the user if the digital identity is valid and to provide a result of the authentication of the user to the external-entity during the electronic transaction, wherein said dynamic code is alphanumeric.

53. The apparatus of claim 52, wherein said external-entity and central-entity are the same entity.

54. The apparatus of claim 52, wherein the user-specific information includes user-identifying information.

55. The method of claim 52, wherein the user-specific information comprises one or more of the following: an alphanumeric name, an ID, a login name, and an identification phrase.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,266,432 B2
APPLICATION NO. : 12/210926
DATED : September 11, 2012
INVENTOR(S) : Nader Asghari-Kamrani et al.

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 (63) - "Continuation of application No. 11/239,046, filed on Sep. 30, 2005, now Pat. No. 7,444,676, which is a continuation of application No. 09/940,635, filed on Aug. 29, 2001, now Pat. No. 7,356,837." should read,

-- Continuation-in-part of application No. 11/239,048, filed on Sep. 30, 2005, now Pat. No. 7,444,676, which is a continuation-in-part of application No. 09/940,635, filed on Aug. 29, 2001, now Pat. No. 7,356,837. Continuation-in-part of application No. 11/333,400, filed on Jan. 18, 2006, now Pat. No. 8,281,129, which is a continuation-in-part of application No. 09/940,635, filed on Aug. 29, 2001, now Pat. No. 7,356,837. --

Item (60) - "Provisional application No. 60/615,603, filed on Oct. 5, 2004." should read,

-- Provisional application No. 60/615,603, filed on Oct. 5, 2004. Provisional application No. 60/650,137 filed on Feb. 7, 2005. --

In the Specification,

Column 1, Lines 6-17 - "This application is a Continuation of application Ser. No. 11/239,046, filed Sep. 30, 2005 now U.S. Pat. No. 7,444,676, with a priority of a U.S. provisional application 60/615,603, filed Oct. 5, 2004, with the same inventors and assignee. This application is also a Continuation of another U.S. application Ser. No. 09/940,635, filed Aug. 29, 2001, and patented as U.S. Pat. No. 7,356,837, on Apr. 8, 2008, titled "Centralized identification and authentication system and method", with the same inventors and assignee. Please note that the current application has the same exact specification and Figures as those submitted with the original application Ser. No. 09/940,635, filed Aug. 29, 2001." should read,

Signed and Sealed this
Twenty-fifth Day of October, 2016

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

-- This application is a Continuation-in-part of application Ser. No. 11/239,046, filed Sep. 30, 2005, now U.S. Pat. No. 7,444,676, which claims the benefit of a U.S. provisional application 60/615,603, filed Oct. 5, 2004, and which is also a Continuation-in-part of application No. 09/940,635, filed Aug. 29, 2001, now Pat. No. 7,356,837. Further, this application is a Continuation-in-part of U.S. patent application Ser. No. 11/333,400, filed Jan. 18, 2006, now U.S. Pat. No. 8,281,129, which claims the benefit of U.S. provisional application No. 60/650,137, filed Feb. 7, 2005, which is also a Continuation-in-part of application No. 09/940,635, filed Aug. 29, 2001, now Pat. No. 7,356,837. Please note that the current application has the same exact specification and Figures as those submitted with the original application Ser. No. 09/940,635, filed Aug. 29, 2001. --