

AUTHENTICATION METHOD

TECHNICAL FIELD

5 The present invention relates generally to an authentication method and an authentication system for application thereof.

Background

10 Rubber stamps for the purpose of authenticating documents in the real world are still a commonplace despite the fact that electronic solutions of document processing and signature exist. A problem arises in the real world is that no single company is able to introduce a method of document authenticity verification. Which has resulted in companies not being able to be truly paperless because in certain business process, documents still need to be verified with a company chop using a rubber stamp. Accordingly, there is a need for a solution to the foregoing issue.

15

Summary

20 In accordance with a first aspect of the invention, there is disclosed an authentication method comprising obtaining a user identifier code associated with a document by a computing device and capturing a machine readable code from a user by the computing device. The machine readable code being generated in response to the user identifier code being obtained by the computing device. The authentication method further comprises authenticating the user identifier code with the machine readable code and applying an image to the document by the computing device in response to the user identifier code and the machine readable code, the image being associated with the user identifier code.

25

30 In accordance with a second aspect of the invention, there is disclosed a machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to obtain a user identifier code associated with a document by a computing device and capture a machine readable code from a user by the computing device. The machine readable code being generated in response to the user identifier code being obtained by the computing device. The plurality of programming

instructions, which when executed, the instructions further causes the machine to authenticate the user identifier code with the machine readable code and apply an image to the document by the computing device in response to the user identifier code and the machine readable code, the image being associated with the user identifier code.

5

Brief Description of the Drawings

For a better understanding of the present disclosure, non-limiting and non-exhaustive embodiments are described in reference to the following drawings. In the drawings, like reference numerals refer to parts through all the various figures unless otherwise specified.

10

FIG. 1 shows a system diagram of an authentication system in accordance with an aspect of the invention;

FIG. 2 shows a data flow diagram of the authentication system of FIG. 1; and

15

FIG. 3 shows a process flow diagram of a authentication method in accordance with an aspect of the invention for implementation by the authentication system of FIG. 1.

20

Detailed Description

An exemplary embodiment of the present invention, an authentication method 100 utilising an authentication system 20, is described hereinafter with reference to FIG. 1 to FIG 3.

5

FIG. 1 depicts an exemplary system architecture of the authentication system 20 that can execute implementations of the present disclosure. The authentication system 20 can include a computing device 22 associated with a user, an NFC (Near Field Communication) device 24 and control computer systems 26. The computing device 22 can communicate with one or more of the control computer systems 26 over a network 28. The control computer systems 26 can each include one or more servers 32 and one or more datastores 34, respectively. In some implementations, the authentication system 20 may represent a client/server system supporting multiple computer systems (e.g., control computer systems 26) including one or more clients that are connectively coupled for communication with one another over the network 30.

15

The computing device 22 can represent various forms of processing devices including, but not limited to, a desktop computer, a laptop computer, a handheld computer, a personal digital assistant (PDA), a smartphone, a smart tablet, a cellular telephone, a network appliance, a camera, a smart phone, an enhanced general packet radio service (EGPRS) mobile phone, a media player, a navigation device, an email device, a game console, or a combination of any two or more of these data processing devices or other data processing devices. The computing device 22 may access application software on one or more of the control computer systems 26.

25

The control computer systems 26 can represent various forms of server systems including, but not limited to a web server, an application server, a proxy server, a network server, or a server farm. For example, one or more of the servers 32 can be an application server that executes software accessed by the computing device 22. In some implementations, a user can invoke applications available on one or more of the servers 32 in a web browser or a

30

mobile application running on a client (e.g., computing device 22). Each application can individually access data from one or more repository resources (e.g., datastores 112).

In some implementations, the computing device 22 may communicate wirelessly through a communication interface (not shown), which may include digital signal processing circuitry where necessary. The communication interface may provide for communications under various modes or protocols, such as Global System for Mobile communication (GSM) voice calls, Short Message Service (SMS), Enhanced Messaging Service (EMS), or Multimedia Messaging Service (MMS) messaging, Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), Personal Digital Cellular (PDC), Wideband Code Division Multiple Access (WCDMA), CDMA2000, or General Packet Radio System (GPRS), among others. For example, the communication may occur through a radio-frequency transceiver (not shown). In addition, short-range communication may occur, such as using a Bluetooth, WiFi, or other such transceiver.

The network 30 can be a large computer network, such as a local area network (LAN), wide area network (WAN), the Internet, a cellular network, or a combination thereof connecting any number of mobile clients, fixed clients, and/or servers. In some implementations, each client (e.g., computing device 22) can communicate with one or more of the control computer systems 26 via a virtual private network (VPN), Secure Shell (SSH) tunnel, or other secure network connection. In some implementations, the network 30 can include the Internet, a wireless service network and may include the Public Switched Telephone Network (PSTN). In other implementations, the network 30 may include a corporate network (e.g., an intranet) and one or more wireless access points.

The computing device 22 can establish its own session with the control computer systems 26. Each session can involve two-way information exchange between the control computer systems 26 and the computing device 22. For example, a Hypertext Transfer Protocol (HTTP) session can allow the association of information with individual users. A session can be stateful session, in which at least one of the communicating parts (e.g., the control

computer systems 26 or the computing device 22) stores information about the session history in order to be able to communicate. Alternatively, stateless communication during a stateless session includes independent requests with associated responses.

5 The authentication method 100, as shown in FIG. 3 and with data flow shown in FIG. 2, comprises obtaining a user identifier code 50 associated with a document 57 by the computing device 22 in a step 102. Next, a machine readable code 52 is captured from a user 54 by the computing device 22 in a step 104. The machine readable code 52 is generated in response to the user identification code 50 being obtained by the computing
10 device 22. The user identifier code 50 is then authenticated with the machine readable code 52 in a step 106. Once the user identifier code 50 has been authenticated with the machine readable code 52 in the step 106, an image 56 is received by the computing device 22 in a step 108. The image 56 is for one of application to or association with the document 57 stored and processable by one of the computing device 22 and a system in data
15 communication with the computing device 22 in a step 110.

Preferably, the computing device 22 comprises at least one of an image capture device and a code scanner for capturing the machine readable code 52. The machine readable code 52 is preferably a 2D barcode, a 3D barcode and a QR code.

20

The step 104 of capturing the machine readable code 52 comprises generating the machine readable code in a step 202, associating the generated machine readable code 52 with the user identifier 50 in a step 204 and providing the machine readable code to a first user device 80 in a step 206. The step 202 of generating the machine readable code 52 can be
25 initiated through the computing device 22 or the first user device 80. Alternatively, the machine readable code 52 is generated in the step 202 in response to the user identification code 50 being obtained in the step 102. Once generated, the machine readable code 52 is at least one of being displayable on the first user device 80, being providable from the first user device to a second user device 82 for display thereon and being printed from the first
30 user device 80 for capture by the computing device 22. The use of the second user device

82 is an option available when the first user device 80 is not in proximity with the computing device 22 and will therefore require assistance of the second user device 82 which happens to be in proximity with the computing device 22. As described, the machine readable code 52 can then be sent from the first user device 80 to the second user device 82
5 for display on the second user device 82 for capture by the computing device 22 therefrom.

Once the user identifier code 50 has been authenticated with the machine readable code 52 in the step 106, the machine readable code 52 is at least one of disassociated from the user identifier code 50 and invalidated in a step 210. Alternatively or additionally, a validity
10 duration, for example a few seconds, may be assigned to the machine readable code 52 which will be invalidated upon expiry of the validity duration. However, the validity duration of the machine readable code 52 may be set to never expire until or even after use thereof for authentication.

15 The step 102 of obtaining the user identifier code 50 associated with the document 57 by a computing device 22 comprises retrieving the user identifier code 50 from a plurality of computer systems in communication with the computing device 22, the plurality of computer systems being specifically the control computer systems 26. Alternatively, the user identifier code 50 is obtained by capturing user entry thereof by the user using the
20 computing device 22.

In a first implementation approach of the authentication method 100, the step 106 of authenticating the user identifier code 50 with the machine readable code 52 comprises sending the user identifier code 50 and the machine readable code 52 to the control
25 computer systems 26 in a step 112. In the first implementation approach, the step 108 of receiving the image 56 by the computing device 22 comprises receiving the image 56 from the control computer systems 26 in a step 114.

In a second implementation approach of the authentication method 100, the step 106 of authenticating the user identifier code 50 with the machine readable code 52 comprises authenticating the user identifier code 50 with the machine readable code 52 by the computing device 22 in a step 122. In the second implementation approach, the step 108 of receiving the image 56 by the computing device 22 comprises receiving the image 56 from the control computer systems 26 in a step 124 in response to the identifier code 50 and the machine readable code 52 being authenticated.

10 In any of the implementation approaches, the image 56 may require decryption using a password provided by the user of a password generated from the machine readable code 52 provided by the user 54 prior to use thereof with the document 57. Decryption of the image 56 can be achieved through use of the machine readable code 52 or a password generated therefrom. Alternatively, the user identifier code 50 and the machine readable code 52 may
15 be sent to the control computer systems 26 for authentication thereby. Upon authentication of the user identifier code 50 and the machine readable code 50 by the control computer systems 26, an authentication code is sent by the control computer systems 26 to the computing device 22 for use in decrypting the image 56. Depending on implementation, the authentication code may be used in isolation or in combination with one or more of the user
20 identifier code 50 and the machine readable code 52 for decrypting the image 56.

It is also herein disclosed that the invention can be implemented as a machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to obtain the user identifier code 50 associated
25 with the document 57 by the computing device 22 and capture a machine readable code 52 from the user 54 by the computing device 22. The machine readable code 52 is generated in response to the user identifier code 50 being obtained by the computing device 22. The plurality of programming instructions, which when executed, the instructions further causes the machine to authenticate the user identifier code 50 with the machine readable code 52
30 and apply the image 56 to the document 57 by the computing device 22 in response to the

user identifier code 50 and the machine readable code 52 being authenticated, with the image 56 being associated with the user identifier code 50.

General Application of Method and System

5

Further details of the present invention are provided hereinafter to the authentication method 100 and the authentication system 20 (“a system” and “a method” respectively) that can be utilized with a variety of different portable communication devices, including but not limited to PDA’s cellular phones, smart phones, laptops, tablet computers and other mobile devices that include cellular data service as preferable access to consumer downloadable applications. One such device could be an iPhone or Samsung S5. The portable communication device technology platform may be Apple OS, Android OS, Microsoft Windows mobile, Microsoft Windows Phone 7, RIM Blackberry OS, Samsung Tizen, Symbian, Java or any other technology platform. For the purposes of this disclosure, the present invention has been generally described in accordance with features and interfaces that are optimized for a smart phone utilizing a general platform that is connected to our system in the cloud, although one skilled in the art would understand that all such features and interfaces may also be used and adapted for any other platform and/or device.

20 A user creates an account with a unique company id on our cloud based platform. After providing authenticity of the legitimacy of the user who is authorized to create such the company id, the admin rights will be assigned to this user.

25 It is preferred that initiation of authentication is facilitated and controlled by the mobile application residing on the mobile communication device with the mobile application managing the first time user registration and authentication, initiation of the authentication process via the mobile application and/or via an authenticated mobile application (preferably residing on another mobile communication device) and managing download and decryption of the image, for example a company stamp image, to be stored in the library residing on the

mobile communication device, applied to an electronic document residing on or being accessed by the mobile communication device.

5 It is preferred that the mobile application and the mobile communication device constitute at least a portion of the authentication system. Further, the authentication system can further comprise the cloud-based platform which the mobile application communicates and interacts with via the mobile communication device.

10 Whenever the method is initiated, a second factor authentication prompt will be triggered by the library which will communicate with our platform in the cloud or embedded software library, whereby it would be required to provide the abovesaid machine readable code, for example a QR code, to verify themselves as an authorized user. The mobile communication device, through interaction with the mobile application, may initiate the generating of the machine readable code for sending to a first user communication device.

15 The machine readable code can then be displayed on the first user communication device for capture by the mobile communication device. Once captured, the machine readable code will then be sent by the mobile communication device to the cloud-based platform for verification by the cloud-based platform. Generating of the machine readable code can also be initiated and requested by the first user communication device. In situations when the

20 user of the first communication device is not at the intended location where the mobile communication device is, the machine readable code can be sent from the first user communication device to a second user communication device which is proximal to the mobile communication device to enable capture of the machine readable code therefrom. The machine readable code is invalidated once authentication has been achieved or at the expiry

25 of a time limit from when it was generated. Each of the first user communication device and the second user authentication device is one of a smart device, a smart phone and a smart tablet.

30 Once authenticated, the digital image of a company stamp would be sent to the library to be superimposed onto, tagged with or merged with the document together with an optional

signatory process (i.e. wet ink signature or electronic image signature). This signed document will be stored back into the cloud for archival and retrieval by verified users if connectivity is present.

- 5 For clarity, the document can be a transactional document, for example a delivery order, which is standalone or associated as a schedule of a master document. Alternatively, the document can be one or more pages or dialog screens of a website, a web application or a mobile application where transaction is effected, for example a check-out page or endorsement page of an e-commerce site. Further alternatively, the document can be a data interface page or a content display page of or a transactional document contained in a business management system, for example an ERP system.

Encrypted Company Stamp

- 15 When a user is successfully authenticated, a digital company stamp will be created containing the company stamp image as well as encapsulated and embedded with the name of the user that authorized the one time use of the stamp as well as timestamp.

The recreated image will be encrypted and sent to the library through the internet from the cloud platform and sent to the software library on the mobile application. Once it reaches the software library, it will be decrypted and embedded in the mobile application or mobile form.

Examples

- 25 In an example of the application of the authentication system, specifically with use of the authentication method, a logistic truck driver carries a tablet containing a mobile application that is embedded with our software library. Here, the tablet functions as the mobile communication device as aforementioned.

When he reaches the customer's place, he will launch the application requesting for the customer's signature and company stamp. The mobile application will present the relevant document, for example a delivery order (DO), for endorsement by the customer. The document will have an associated user identifier code that is retrievable by the tablet (i.e. the computing device) through, for example, a cloud-based system (i.e. the control computer systems).

The customer has pre-registered for use of the authentication method and will be provided with a machine readable code with an associated user identifier code. The customer would also have provided an image of the stamp (i.e. company stamp) for upload to the cloud-based system.

The cloud-based system may provide specific software applications for instantaneous generation or design of the image should the image be unavailable for upload to the cloud-based system. The mobile application will prompt the customer (i.e. the user) for a machine readable code, or with an additional option to provide a password, which is to be captured by the tablet. Initiating generation of the machine readable code can be requested through the mobile application operating on the tablet or using an associated mobile application on a first user device. Once requested, the cloud-based platform will generate and send a one-time, limited duration or limited times use machine readable code to the first user device which is associated with the DO. The machine readable code is then displayed on the first user device for capture by the tablet using an image capture module thereof. If the intended user, and consequently the first user device, is not at the customer location, the machine readable code can be sent to a second user device held by a friend or colleague so that it may be displayed for capture by the tablet. The machine readable code is authenticated with the user identifier code by either the tablet or the cloud-based system. In this instance, the computing device 22 in the step 104 is the tablet while the user 54 is the customer. Alternatively, the machine readable code may instead be provided to for display on the tablet to enable capture of the displayed machine readable code by the first user device for authentication thereof. Meta-data may be embedded in the machine readable code for, for

example, indicating or describing the user identifier code, the DO code and/or links to the user identifier code, the DO code. In this alternative instance, the computing device 22 in the step 104 is the first user device carried by the customer while the user 54 becomes the delivery truck driver.

5

Once positively authenticated, an image containing the corresponding company stamp is sent from the cloud-based system to the tablet for application of the image to the DO. Alternatively, the image may be downloaded together with the DO from the cloud-based system onto the tablet prior to capture of the machine readable code from the customer. The image will be decrypted and applied to the DO only upon successful capture and authentication of the machine readable code. Further alternatively, the user identifier code may be provided by the customer instead of being retrieve automatically based on association with the DO. The mobile application may further request capture of the customer's signature based on preference. The final DO endorsed with the image of the company stamp may be sent to the cloud-based system for archival purpose.

10
15

In another example of the application of the authentication system, specifically with use of the authentication method in a B2C context, a healthcare personnel at a medical facility carries a smart device containing a mobile application that is embedded with our software library. Here, the smart device functions as the mobile communication device as aforementioned.

20

When the healthcare personnel approaches a patient, or potential patient, of the healthcare facility requesting consent for health records of the patient be made accessible by the medical facility and/or be shared by the medical facility with third party individuals or institutions, the healthcare personnel will present the consent document to the patient for endorsement. Endorsement of such consent documents are usually effected by signature. However, signatures, captured in wet-ink or a signature-pad, are ineffective against abuse and forgeries. Further, genuine consent of such documents are usually difficult to track or can remained untracked.

25
30

Hence, with the authentication method, the healthcare personnel not only presents the consent document to the patient using the smart device for capturing signature of the patient to indicate consent, but is also required to place a virtual stamp on the consent document.

5

Hence, in accordance with the authentication method, the healthcare personnel will launch the application requesting for the patient's signature and company stamp. The mobile application will present the relevant document, for example the consent document, for endorsement by the patient. The patient may be required to provide the user identifier code thereof to enable the relevant document to be retrieved by the smart device, or the document will have an associated user identifier code that is retrievable by the smart device tablet (i.e. the computing device) through, for example, a cloud-based system (i.e. the control computer systems).

10

15 The patient has pre-registered for use of the authentication method and will be provided with a machine readable code, when required, with an associated user identifier code. The patient would also have provided an image of the stamp (i.e. company stamp) for upload to the cloud-based system.

20 The cloud-based system may provide specific software applications for instantaneous generation or design of the image should the image be unavailable for upload to the cloud-based system. The mobile application will prompt the patient (i.e. the user) for a machine readable code which the patient will provide through a user device belonging to the patient for capture by the smart device tablet. The machine readable code is authenticated with the
25 user identifier code by either the smart device or the cloud-based system.

Once positively authenticated, an image containing the corresponding personal stamp is sent from the cloud-based system to the smart device for application of the image to the consent document. Alternatively, the image may be downloaded together with the consent
30 document from the cloud-based system onto the smart device prior to capture of the

machine readable code from the user device of the patient. The image will be decrypted and applied to the consent document only upon successful capture and authentication of the machine readable code. Further alternatively, the user identifier code may be provided by the patient instead of being retrieve automatically based on association with the consent document. The mobile application may further request capture of the patient's signature based on preference. The final consent document endorsed with the image of the personal stamp may be sent to the cloud-based system for archival purpose. Further, an alert to the applying of the stamp onto the document will be sent to contact points of the patient, for example through emails or messaging communication platforms, to bring use of the stamp to the attention of the patient.

Aspects of particular embodiments of the present disclosure address at least one aspect, problem, limitation, and/or disadvantage associated with existing computer-implemented methods and systems. While features, aspects, and/or advantages associated with certain embodiments have been described in the disclosure, other embodiments may also exhibit such features, aspects, and/or advantages, and not all embodiments need necessarily exhibit such features, aspects, and/or advantages to fall within the scope of the disclosure. It will be appreciated by a person of ordinary skill in the art that several of the above-disclosed structures, components, or alternatives thereof, can be desirably combined into alternative structures, components, and/or applications. In addition, various modifications, alterations, and/or improvements may be made to various embodiments that are disclosed by a person of ordinary skill in the art within the scope of the present disclosure, which is limited only by the following claims.

Claims

1. An authentication method comprising:
 - obtaining a user identifier code associated with a document by a computing device;
 - 5 capturing a machine readable code from a user by the computing device;
 - generating the machine readable code;
 - associating the generated machine readable code with the user identifier;
 - and
 - providing the machine readable code to a first user device,
 - 10 wherein the machine readable code at least one of being displayable on the first user device, being providable from the first user device to a second user device for display thereon and being printed from the first user device for capture by the computing device, the machine readable code being generated in response to the user identifier code being obtained by the computing device;
 - 15 authenticating the user identifier code with the machine readable code; and
 - applying an image to the document by the computing device in response to the user identifier code being authenticated with the machine readable code, the image being associated with the user identifier code.
- 20 2. The authentication method as in claim 1, the computing device comprising at least one of an image capture device and a code scanner for capturing the machine readable code.
3. The authentication method as in claim 1, the machine readable code being a 2D
 - 25 barcode, a 3D barcode and a QR code.
4. The authentication method as in claim 1, further comprising:
 - at least one of disassociating the machine readable code from the user identifier code and invalidating the machine readable code in response to the user

identifier code being authenticated with the machine readable code captured by the computing device.

5. The authentication method as in claim 1, obtaining a user identifier code associated with a document by a computing device comprising one of:

retrieving the user identifier code from a plurality of computer systems in communication with the computing device and capturing user data entry of the user user identifier code by the user using the computing device.

6. The authentication method as in claim 1, applying an image to the document by the computing device comprising:

one of application to or association of the image with a document stored and processable by one of the computing device and a system in data communication with the computing device.

7. The authentication method as in claim 1, authenticating the identifier code with the machine readable code comprising:

sending the user identifier code and the machine readable code to a plurality of computer systems for authentication thereby.

8. The authentication method as in claim 7, receiving an image by the computing device in response to the identifier code and the machine readable code being authenticated comprising:

receiving the image from the plurality of computer systems.

9. The authentication method as in claim 7, authenticating the identifier code with the machine readable code further comprising:

receiving an authentication code from the plurality of computer systems by the computing device in response to the user identifier code and the machine readable code being authenticated

10. The authentication method as in claim 9, authenticating the user identifier code with the password further comprising:

5 decrypting the image using the authentication code by the computing device for subsequent application of the image to the document.

11. The authentication method as in claim 6, further comprising:

10 decrypting the image using a password generated from the machine readable code by the computing device for subsequent application of the image to the document.

12. A machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to:

15 obtain a user identifier code associated with a document by a computing device;

 capture a machine readable code from a user by the computing device, the machine readable code being generated in response to the user identifier code being obtained by the computing device;

20 generating the machine readable code;

 associating the generated machine readable code with the user identifier;

 providing the machine readable code to a first user device;

 authenticate the user identifier code with the machine readable code; and

25 apply an image to the document by the computing device in response to the user identifier code being authenticated with the machine readable code, the image being associated with the user identifier code,

30 wherein the machine readable code at least one of being displayable on the first user device, being providable from the first user device to a second user device for display thereon and being printed from the first user device for capture by the computing device.

13. The machine-readable medium as in claim 12, wherein the computing device comprising at least one of an image capture device and a code scanner for capturing the machine readable code.
- 5 14. The machine-readable medium as in claim 12, the machine readable code being a 2D barcode, a 3D barcode and a QR code.
15. The machine-readable medium as in claim 12, further comprising:
10 at least one of disassociating the machine readable code from the user identifier code and invalidating the machine readable code in response to the user identifier code being authenticated with the machine readable code captured by the computing device.
- 15 16. The machine-readable medium as in claim 12, wherein obtaining a user identifier code associated with a document by a computing device comprises one of:
retrieving the user identifier code from a plurality of computer systems in communication with the computing device and capturing user data entry of the user user identifier code by the user using the computing device.
20
17. The machine-readable medium as in claim 12, wherein applying an image to the document by the computing device comprises:
one of application to or association of the image with a document stored and processable by one of the computing device and a system in data communication
25 with the computing device.
18. The machine-readable medium as in claim 12, further comprising:
decrypting the image using the password generated from the machine readable code by the computing device for subsequent application of the image to the
30 document.

19. The machine-readable medium as in claim 12, authenticating the identifier code with the machine readable code comprising:

5 sending the user identifier code and the machine readable code to a plurality of computer systems for authentication thereby;

receiving an authentication code from the plurality of computer systems by the computing device in response to the user identifier code and the machine readable code being authenticated; and

10 decrypting the image using the authentication code by the computing device for subsequent application of the image to the document.

AUTHENTICATION METHOD

5 Abstract

Described herein is a method comprising obtaining a user identifier code associated with a document and capturing a machine readable code from a user. The method further comprising authenticating the user identifier code with the machine readable code and applying an image to the document in response to the identifier code and the machine

10 readable code being authenticated.

15

Figure 1