

AUTHENTICATION SYSTEM AND METHOD

TECHNICAL FIELD

5 The present invention relates generally to the use of NFC combined in a device, for example a Rubber Stamp, a credit card, as a trigger for authentication with a cloud-based platform or software library whereby it will authorize the user to be able to securely sign documents even when taking an offline method after an initial pairing process that is connected to the cloud gateway for the first time.

10 Background

The usage of NFC has become common place in the market. 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.

15 Near Field Communication (NFC) is a technology that uses electromagnetic waves to exchange data. NFC waves are transmitted over a short-range (on the order of a few inches) and at high-frequencies. NFC devices are already being used to make payments at point of sale devices. NFC is an open standard (see, e.g. ISO/IEC 18092) specifying modulation schemes, coding, transfer speeds and RF interface. There has been wider adoption of NFC
20 as a communication platform because it proves better security for financial transactions and access control.

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
25 truly paperless because in certain business process, documents still need to be verified with a company chop using a rubber stamp.

Accordingly, the present invention seeks to resolve this problem by redefining the usage of the rubber stamp or the like objects as an authentication device by having an embedded NFC
30 tag in the stamp.

Summary

In accordance with a first aspect of the invention, there is disclosed an authentication method comprising receiving a chip identifier code from an NFC device by a computing device and receiving a password from a user by the computing device. The authentication method further comprises authenticating the chip identifier code with the password and receiving an image by the computing device in response to the identifier code and the password being authenticated. The image is for one of application to or association with a document stored and processable by one of the computing device and a system in data communication with the computing device.

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 receive a chip identifier code from an NFC device by a computing device and receive a password from a user by the computing device. The plurality of programming instructions, when executed, further cause the machine to authenticate the chip identifier code with the password and receive an image by the computing device in response to the identifier code and the password being authenticated. The image is for one of application to or association with a document stored and processable by one of the computing device and a system in data communication with the computing device.

In accordance with a third aspect of the invention, there is disclosed an authentication system for utilizing an embedded NFC chip couplable with an object for authenticating a document, the authentication system comprising a mobile communication system. The mobile communication device comprises a controller executing a mobile application to enable initiation of an authentication process via at least one of detecting proximity of the NFC chip with the mobile communication device and initiation by a user by interaction thereof with the mobile communications device, the authentication process for prompting

for a password from the user and at least one of a user id from the user and an NFC chip id from the NFC chip, the password and at least one of the NFC chip id and the user id being providable to a cloud platform or a software library embedded in the mobile application for authentication thereby. An embedded image stored in the nfc chip is receivable from the
5 loud-based platform or the software library upon positive authentication of the password and at least one of the NFC chip id and the authenticated user id thereby for one of application to or association with the document stored and processable by one of the mobile communication device and a system in data communication with the mobile communication device.

10

In accordance with a fourth aspect of the invention, there is disclosed a system for utilizing an embedded NFC chip in a rubber stamp for authenticating and verifying documents through a 2FA process that is connected to a cloud platform or communicates with the software library that is embedded in the mobile application and also comprising a secure
15 element operably connected to the NFC baseband; and a unique authentication id stored in the secured element.

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
5 reference numerals refer to parts through all the various figures unless otherwise specified.

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

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

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;

15

FIG 4. shows a system diagram of the authentication system of FIG. 1 utilizing the authentication method of FIG. 3 executed between the embedded NFC chip in the rubber stamp with the platform in the cloud in accordance to an aspect of the invention;

20 FIG 5. shows a system flow diagram of the authentication system of FIG. 4 with option of two actions that can be triggered by the embedded library in the mobile application;

FIG 6. shows a system flow diagram of one of the options of the authentication method/process of FIG. 5 that can be triggered by the NFC-Enabled Rubber Stamp; and

25

FIG 7. Shows a system flow diagram of the other of the options of the authentication method/process of FIG. 5 that can be triggered by the authenticated mobile application.

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 7.

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 receiving a chip identifier code 50 from the NFC device 24 by the computing device 22 in a step 102. Next, a password 52 is received from a user 54 by the computing device 22 in a step 104. The chip identifier code 50 is then authenticated with the password 52 in a step 106. Once the chip identifier code 50 has been authenticated with the password 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 a document 57 stored and processable by one of the computing device 22 and a system in data communication with the computing device 22 in a step 110.
- 10
- 15 In a first implementation approach of the authentication method 100, the step 106 of authenticating the chip identifier code 50 with the password 52 comprises sending the chip identifier code 50 and the password 52 to the control 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.
- 20

- In a second implementation approach of the authentication method 100, the step 106 of authenticating the chip identifier code 50 with the password 52 comprises receiving an authentication code 58 from the control computer systems 26 by the computing device 22 in response to the identifier code and the password being authenticated in a step 116. In the second implementation approach, the step 108 of receiving the image 56 by the computing device 22 comprises sending the authentication code 58 to the NFC device 24 in a step 118 and receiving the image 56 from the NFC device 24 by the computing device 22 in a step 120 in response to the authentication code 58 being sent thereto.
- 25

In a third implementation approach of the authentication method 100, the step 106 of authenticating the chip identifier code 50 with the password 52 comprises authenticating the chip identifier code 50 with the password 52 by the computing device 22 in a step 122. In the third implementation approach, the step 108 of receiving the image 56 by the computing device 22 comprises receiving the image 56 from the NFC device 24 in a step 124 in response to the identifier code 50 and the password 52 being authenticated.

In a fourth implementation approach of the authentication method 100, the step 106 of authenticating the chip identifier code 50 with the password 52 comprises authenticating the chip identifier code 50 with the password 52 by the computing device 22 in a step 126. In the fourth implementation approach, the step 108 of receiving the image 56 by the computing device 22 comprises sending an authentication code 60 to the NFC device 24 by the computing device 22 in a step 128 in response to the identifier code 50 and the password 52 being authenticated, and receiving the image 56 from the NFC device 24 in a step 130 in response to the authentication code 60 being sent to the NFC device 24.

In any of the implementation approaches, the image 56 may require decryption using the password 52 provided by the user 54 prior to use thereof with the document 57.

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 receive the chip identifier code 50 from the NFC device 24 by the computing device 22 and receive the password 52 from the user 54 by the computing device 22. The plurality of programming instructions, when executed, further cause the machine to authenticate the chip identifier code 50 with the password 52 and receive the image 56 by the computing device 22 in response to the identifier code 50 and the password 52 being authenticated. 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 communication with the computing device 22.

Embedded NFC chip in a device (for example a Rubber Stamp)

With further reference to FIG. 4 to FIG. 7, 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.

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.

The NFC chip that is embedded in a device, for example in a traditional rubber stamp, in a credit card, in a substrate attachable to objects and the like adaptations, would first be authenticated for first time use using a mobile application download to the mobile device with NFC capabilities or a computer that has a NFC reader. The purpose of this application is to pair the unique id stored in the NFC chip with the company id keyed in by the user on the application.

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 use registration and authentication, initiation of the authentication process via proximal interaction/signal communication of the NFC chip with the mobile communication device, 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 or on NFC secure element itself.

- 10 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. Further, this invention covers the ability for the stamp to be utilized in an environment where there is no internet connectivity
- 15 after the initial pairing process.

The admin user would be able to assign different users to have the rights to use this particular stamp to authenticate and verify documents with their unique pin.

- 20 Whenever the stamp is used by touching a NFC enabled mobile communication device that is embedded with the software library provided to them by us, 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 they would be required to enter their pin to verify themselves as an authorized user. This pin will be sent with the authentication id and
- 25 company id for verification by the cloud-based platform. Alternatively, the pin will be used used to verify that the user that is utilizing the nfc digital stamp is an authorized user, with the verification process occurs on the software library.

Once authenticated, the digital image of the 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).

- 5 This signed document will be stored back into the cloud for archival and retrieval by verified users if connectivity is present.

Authenticated Mobile Application

10

An alternative authentication method exists as shown in FIG. 4. A user has to pair a mobile device to the cloud platform with the company id using the mobile authentication application.

- 15 When a user selects the option of “Authentication through mobile application” as shown in FIG. 5 and FIG. 7, the user is prompted by the library to enter the company id into the mobile application.

- 20 A push notification will be triggered to the mobile authenticated device that is paired to the company id. This will result in an authentication process that is triggered by the system. A push notification will be sent to the mobile authenticated device. This will trigger a prompt by the application to request for an authentication pin by the user. Once the correct pin is entered into the system, the cloud platform will push the encrypted company image to the mobile application that is embedded by our library.

25

30

Encrypted Company Stamp

When a user is successfully authenticated through FIG. 6 or FIG. 7, a digital company stamp will be created containing the company stamp image as well as encapsulated and embedded
5 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
10 form.

Examples

In an example of the application of the authentication system, specifically with use of the NFC chip, and the authentication method, a logistic truck driver carries a tablet containing a
15 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.
20

There are two situations that can take place (or two options to be selectable):

Situation 1: (Customer selects "Authenticate through NFC Enabled Stamp" <See figure 6>

25 The customer will use the NFC enabled Stamp and touch the NFC enabled Tablet containing our mobile application that is embedded with our software library. This will trigger a process whereby the software library will request for the customer's pin. The company id, NFC unique id, customer's pin will be encrypted and sent to the cloud for authentication.

30

If the details are successfully authenticated, the company stamp image will be sent from the cloud embedded with the user name as well as timestamp to the software library to be superimposed onto the electronic document in the mobile application or the mobile form.

5 Situation 2: (Customer selects “Authenticate through Mobile authenticated Device” <See figure 7>

10 A push notification will be sent to the mobile authenticated device that was paired to the company id. The customer can launch the app to approve the one time usage of the digital company stamp.

15 The application will prompt for a pin verification. Once the user is successfully authenticated, the cloud platform will push the encrypted image embedded with the user’s name and timestamp details to the software library on the mobile application that triggered this process.

Situation 3: (Customer selects “Authenticate through NFC Enabled Stamp” <See figure 6>

20 The customer will use the NFC enabled Stamp and touch the NFC enabled Tablet containing our mobile application that is embedded with our software library. This will trigger a process whereby the software library will request for the customer’s pin. The company id, nfc unique id, customer’s pin will be encrypted and processed and authenticated by the software library embedded in the mobile application.

25 If the details are successfully authenticated, the company stamp image will be extracted from the NFC secure element which contains the embedded image, after a successful authentication, the image as well as the username and timestamp will be superimposed onto the electronic document in the mobile application or the mobile form.

Authentication is preferably performed by the mobile application which completes the authentication positively through sending an instruction to or an authentication code to the NFC secure element which in response, will send the image to the mobile application executing on the computing device, via the software library. The image received by the
5 computing device via the mobile application may be used as is for application with the document, or may require further decrypting using the password already received from the user.

Aspects of particular embodiments of the present disclosure address at least one aspect,
10 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
15 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
20 the following claims.

Claims

1. An authentication method comprising:

receiving a chip identifier code from an NFC device by a computing device;

receiving a password from a user by the computing device;

- 5 authenticating the chip identifier code with the password; and

receiving an image by the computing device in response to the identifier code and the password being authenticated,

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

10

2. The authentication method as in claim 1, further 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.

15

3. The authentication method as in claim 1, authenticating the identifier code with the password comprising:

sending the chip identifier code and the password to a plurality of computer systems for authentication thereby.

20

4. The authentication method as in claim 3, receiving an image by the computing device in response to the identifier code and the password being authenticated: receiving the image from the plurality of computer systems.

25

5. The authentication method as in claim 3, authenticating the identifier code with the password further comprising:

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

30

6. The authentication method as in claim 5, receiving an image by the computing device in response to the identifier code and the password being authenticated:
 - 5 sending the authentication code to the NFC device; and
 - receiving the image from the NFC device by the computing device in response to the authentication code being sent thereto.
7. The authentication method as in claim 1, authenticating the identifier code with the password comprising:
 - 10 authenticating the identifier code with the password by the computing device.
8. The authentication method as in claim 7, receiving an image by the computing device in response to the identifier code and the password being authenticated:
 - 15 receiving the image from the NFC device in response to the identifier code and the password being authenticated.
9. The authentication method as in claim 7, receiving an image by the computing device in response to the identifier code and the password being authenticated:
 - 20 sending an authentication code to the NFC device by the computing device in response to the identifier code and the password being authenticated; and
 - receiving the image from the NFC device in response to the authentication code being sent to the NFC device.
10. The authentication method as in claim 2, further comprising:
 - 25 decrypting the image using the password by the computing device.

11. A machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to:
- 5 receive a chip identifier code from an NFC device by a computing device;
 receive a password from a user by the computing device;
 authenticate the chip identifier code with the password; and
 receive an image by the computing device in response to the identifier code and the password being authenticated,
- 10 wherein the image is for one of application to or association with a document stored and processable by one of the computing device and a system in data communication with the computing device.
- 15 12. The machine-readable medium as in claim 11, wherein 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.
- 20 13. The machine-readable medium as in claim 12, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
 send the chip identifier code and the password to a plurality of computer systems for authentication thereby.
- 25 14. The machine-readable medium as in claim 13, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
 receive the image from the plurality of computer systems.

15. The machine-readable medium as in claim 13, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
- 5 receive an authentication code from the plurality of computer systems by the computing device in response to the identifier code and the password being authenticated
16. The machine-readable medium as in claim 15, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
- 10 send the authentication code to the NFC device; and
receive the image from the NFC device by the computing device in response to the authentication code being sent thereto.
17. The machine-readable medium as in claim 11, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
- 15 authenticate the identifier code with the password by the computing device.
18. The machine-readable medium as in claim 17, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
- 20 receive the image from the NFC device in response to the identifier code and the password being authenticated.
19. The machine-readable medium as in claim 17, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
- 25 send an authentication code to the NFC device by the computing device in response to the identifier code and the password being authenticated; and
receive the image from the NFC device in response to the authentication code being sent to the NFC device.

20. The machine-readable medium as in claim 12, wherein the plurality of programming instructions, which when executed, the instructions further cause the machine to:
decrypt the image using the password by the computing device.

- 5 21. An authentication system for utilizing an embedded NFC chip couplable with an object for authenticating a document, the authentication system comprising
a mobile communication device comprising a controller executing a mobile application to enable initiation of an authentication process via at least one of
detecting proximity of the NFC chip with the mobile communication device and
10 initiation by a user by interaction thereof with the mobile communications device, the authentication process for prompting for a password from the user and at least one of a user id from the user and an NFC chip id from the NFC chip, the password and at least one of the NFC chip id and the user id being providable to a cloud platform for authentication thereby,
15 wherein an image is receivable from the cloud platform upon positive authentication of the password and at least one of the NFC chip id and the user id thereby for one of application to or association with the document stored and processable by one of the mobile communication device and a system in data communication with the mobile communication device.
- 20 22. The authentication system as in claim 21, the object being one of a rubber stamp, a credit card and a substrate couplable to other objects.
23. A system for utilizing an embedded NFC chip in a rubber stamp for authenticating
25 and verifying documents through a 2FA process that is connected to a cloud platform, the system comprising:
a. A secure element operably connected to the NFC baseband; and
b. A unique authentication id stored in the secured element.