

**Title of the Invention**

Method and System to Capture and Validate a Signature Using a Mobile Device

**5 Cross-Reference to Related Applications**

[0001] The present patent application claims the benefits of priority of United States of America Patent Application No. 61/526,826, entitled "Method and System to Capture and Validate a Signature Using a Mobile Device" and filed at the United States Patent and Trademark Office on August 24, 2011, the content of which is  
10 incorporated herein by reference.

**Field of the Invention**

15 [0002] The present invention generally relates to methods and systems to capture and validate signatures on electronic devices.

**Background of the Invention**

20 [0003] Many items, such as, but not limited to, those for credit and debit card payments, legal and non-legal documents, legal contracts, mortgage documents and other types of items that require a signature are presently done by the signee physically signing his signature to the item.

25 [0004] Current processing for collecting a signature is inconvenient and time consuming for both the company and the signee. Attempts to introduce more automated means have led to more inconvenience and increased cost due, in part, to the requirement of fax machines, signature devices and/or dedicated telephone lines. Most attempts still do not reduce the time it takes to capture a signature for a  
30 company's item.

[0005] Thus, there is a need to adapt new and evolving technologies to provide a much simpler method of capturing a signature for a company's item.

## Summary of the Invention

[0006] A method and a system in accordance with the principles of the present invention generally mitigate at least some shortcomings of prior art methods and systems by allowing the required signature to be captured on a mobile device which can be remote from the item or items requiring a signature.

[0007] Hence, a method to capture and validate a signature, in accordance with the principles of the present invention, generally comprises three main stages.

[0008] In the first stage, the method generally comprises creating a user account on the company's or merchant's server and then displaying or transmitting instructions to the signee on how to capture his signature using his mobile device.

[0009] In the context of the present method and system, a mobile device is a device having access to a communication network and which comprises a touch sensitive screen. Non-limitative examples of such mobile devices include smart phones (e.g. iPhone™, iPod™ Touch, etc.), tablet computers (e.g. iPad™, etc.).

[0010] Understandably, if the signee is on the company's premises, the instructions can be simply display to him. Otherwise, if the signee is at a remote location, the instructions will be transmitted to him, typically, but not exclusively, by email. Other methods of transmission could also be used.

[0011] Once the first stage is done, the method typically proceeds to the second stage in which the method generally comprises prompting the signee to log in his user account and then capture his signature by using his finger (or fingers) or a stylus on the touch sensitive screen of his mobile device. Once the signature is captured, it is transmitted to a secure validation server where it is compared to previously captured signature in order to determine whether or not the captured signature is forged.

[0012] The comparison of the captured signature with previously captured signatures can be performed using available calligraphy analysis tools.

[0013] In some embodiments, the comparison can be performed by third parties.

[0014] If the validation server determines that the captured signature is possibly forged, further analyses can be performed by a human operator.

5

[0015] Ultimately, if the captured signature is validated, the company or merchant will be notified that the captured signature can be retrieved. Otherwise, the company or merchant will be notified that the captured signature is forged and the company or merchant will be prevented from retrieving the captured signature.

10

[0016] The transmittal of notifications to the company or merchant is made between the validation server and the company's or merchant's server via a communication network (e.g. the Internet, a cellular network, etc.).

15 [0017] Finally, in the third stage, the company or merchant will retrieve the captured signature from the validation server and will store it in its server, in association with the item or items that needed a signature, and will notify the signee that the item or items have been signed.

20 [0018] Understandably, the method can comprise other steps or stages as needed.

[0019] In addition, though the company's or merchant's server and the validation server are typically distinct, in other embodiments, both servers could be the same if, for instance, the items' accounts and the signees' account, and the validation are  
25 respectively stored and performed on the same server.

[0020] By allowing a signee to remotely sign an item using his mobile device, the method and system in accordance with the principles of the present invention minimizes the need for a signee to be physically present to sign an item.

30

[0021] Other and further aspects and advantages of the present invention will be obvious upon an understanding of the illustrative embodiments about to be described or will be indicated in the appended claims, and various advantages not referred to

herein will occur to one skilled in the art upon employment of the invention in practice.

### **Brief Description of the Drawings**

5

[0022] The above and other objects, features and advantages of the invention will become more readily apparent from the following description, reference being made to the accompanying drawings in which:

10 [0023] Figure 1 is a flow chart of a portion of the method to capture and validate a signature using a mobile device in accordance with the principles of the present invention.

[0024] Figure 2 is a flow chart of another portion of the method to capture and validate a signature using a mobile device in accordance with the principles of the present invention.

15 [0025] Figure 3 is a flow chart of still another portion of the method to capture and validate a signature using a mobile device in accordance with the principles of the present invention.

[0026] Figure 4 is a schematic diagram of a system in accordance with the principles of the present invention.

20

### **Detailed Description of the Preferred Embodiment**

25 [0027] A novel method and a related system for capturing and validating a signature using a mobile device will be described hereinafter. Although the invention is described in terms of specific illustrative embodiments, it is to be understood that the embodiments described herein are by way of example only and that the scope of the invention is not intended to be limited thereby.

30 [0028] Broadly, the method 10 for capturing and validating a signature using a mobile device comprises several steps which are more or less partitioned in several stages. For instance, in the present embodiment, the method 10 generally comprises three main stages 100, 200 and 300. The different stages generally concern different periods in the overall process of capturing and validating a signature using a mobile device.

[0029] In accordance with the principles of the present invention, a mobile device is a device having access to a communication network (e.g. the Internet, a cellular network, etc.) and which comprises a touch sensitive screen. Non-limitative examples of mobile devices include smart phones comprising touch sensitive screens and tablet computers comprising touch sensitive screens.

[0030] Referring now to Fig. 1, the first stage 100 of the method 10 will be described in more details.

10 [0031] The first stage 100 of the method 10 generally encompasses the creating of an account and the displaying or transmitting of instructions on how to sign using the mobile device.

15 [0032] More specifically, the first stage 100 starts, at 110, by the creation, by a company, a merchant, or any other party (hereinafter “merchant”), of an item that needs the signature of a signee, typically, but not exclusively a customer. Non-limitative examples of other parties include notaries, mortgage lenders, insurance companies, lawyers, etc. Also, the term “item” must be construed broadly to include documents, transactions, approval, debit notes, etc.

20 [0033] Then, at 120, the merchant verifies whether it has established an account for the customer. If an account does exist for the customer, i.e. the account has already been established, then the merchant retrieves, at 130, a unique code from a database located on its server, the unique code being associated with the customer and its account.

25 [0034] If no account has yet been established for the customer, the merchant, at 140, performs an API call to a validation server to create a new customer account and to generate a new unique code. Then, at 150, the validation server, having created the new account and generated the unique code associated with the new account, transmits back the unique code to the merchant. The unique code received by the merchant is then stored in the merchant database at 160 for future retrieval (e.g. step 130).

[0035] Once the unique code has been retrieved, the merchant then performs, at 170, an API call to the validation server to create a new pending item. After that, depending on whether the customer is on the merchant's premises, the merchant can either show the customer how to sign the pending item using his mobile device (at 180) or can send instructions to the customer, typically via email, on how to sign the pending item using his mobile device (at 190).

[0036] Once the first stage 100 is completed, the customer has an account with the merchant and has been shown or instructed on how to sign the pending item using his mobile device.

[0037] Referring now to Fig. 2, the second stage 200 will be described in more details.

[0038] The second stage 200 generally encompasses the actual capture of the signature of the customer using his mobile device. In that sense, after the customer has installed the signature application on his mobile device, the application will prompt the customer, at 210, to enter his unique code, his email address and his password (collectively referred to as his credential information).

[0039] Then, at 220, the application will perform an API call to the validation server to validate the credential information submitted by the customer and to retrieve the pending item(s) that need to be signed.

[0040] Once retrieved, the pending items will be displayed on the screen of the customer's mobile device. In the present embodiment, the pending items are typically displayed as a list, allowing the customer to easily see most, if not all, pending items. The customer can thus choose which item or items he wants to sign. In that sense, it is to be understood that the list of pending items can include items from different merchants if several merchants are registered with the validation server.

[0041] If only one item needs to be signed, then the sole item will be displayed.

[0042] Then, at 230, the customer will first select one or more pending items that need its signature, and will then uses his finger (or fingers) or a stylus and the touch sensitive screen of its mobile device to have his signature captured. In the present embodiment, the application will typically prompt the customer to enter his signature via a specific display. In the present embodiment, the customer can restart the capture of his signature if, for instance, the signature was improperly entered on the touch sensitive screen.

[0043] Once the customer's signature has been properly captured, the application will transmit the captured signature to the validation server (at 240). At this point, the customer does not need to perform other actions. However, the second stage 200 continues to 250 where the validation server, having received the captured signature, validates it against previously captured signatures, if any, stored on the validation server. This validation is performed in order to screen out possibly forged signatures.

[0044] Then, at 260, if it is determined that the captured signature is potentially forged, the validation server will place the item or items in alert and will prevent the merchant from retrieving the signature until the signature has been validated by a human operator.

[0045] At 270, the human operator will determine whether or not the captured signature is forged. This determination can be made with the assistance of signature analysis tools or calligraphy analysis tools. Such tools are available.

[0046] If the human operator determines that the captured signature is not forged, i.e. the captured signature is valid, then the second stage 200 will proceed at 280 where the server will remove the alert on the item or items and will allow the merchant to retrieve the captured signature.

[0047] Otherwise, if the human operator determines that the captured signature is forged, then the second stage 200 will proceed at 290 where the server will notify the merchant that captured signature is forged.

[0048] Though not shown in Fig. 2, when it is determined that a signature is forged, a warning email will typically be sent to the customer's email address in order to inform him that there has been an attempt to forge his signature. Also, the customer's account could possibly be frozen until the forgery attempt has been properly taken care of.

[0049] At this point, the method 10 will typically proceed to the third stage 300 which is illustrated in Fig. 3 in greater details. The third stage 300 typically encompasses the retrieval of the captured signature and the completion of the signing of the item or items.

[0050] Hence, once the validation server has notified the merchant that it is allowed to retrieve the captured signature (step 280), the merchant will make an API call to the validation server, at 310, to actually retrieve the signature for the pending item or items.

[0051] As the validation server receives the retrieval request at 320, it will perform a look-up in the database to fetch the signature, if available, and will then transmit the signature back to the merchant.

[0052] Then, at 330, as the merchant receives the signature from the validation server, the merchant will store the signature within its database and will associate the signature with the pending item or items.

[0053] Then, at 340, the merchant will notify the customer, directly or through an email, that the pending item or items have been signed.

[0054] Understandably, though the three stages 100, 200 and 300 of the method could be performed in one continuous sequence, they could also be performed in a discontinuous sequence. For instance, the first stage 100 could be performed on a given day, the second stage 200 could be performed the next day or even later, and the third stage 300 could be performed some days after the second stage 200 is completed.

[0055] Hence, the method 10 in accordance with the principles of the present invention generally allows a more convenient way of having item signed by avoiding the need for the customer to be physically present and by avoiding the need for the whole signing sequence to be performed in a continuous fashion.

5

[0056] Referring now to Fig. 4, an example of a system 400 allowing the method described above to be performed is depicted.

10

[0057] The system 400 generally comprises a merchant server 410 comprising a computer system 412 and a database 414, a typically remote validation server 420 comprising a computer system 422 and a database 424, at least one mobile device 430 comprising a touch-sensitive screen (three are shown), and a communication network 440 (e.g. the Internet, a cellular network, etc.) which allows communication between the merchant server 410, the validation server 420 and the at least one mobile device 430.

15

[0058] Understandably, as the various stages of the method 10 are performed, information, requests, and API calls will be transmitted between the servers 410 and 420 and the at least one mobile device 430 through the communication network 440.

20

[0059] While illustrative and presently preferred embodiments of the invention have been described in detail hereinabove, it is to be understood that the inventive concepts may be otherwise variously embodied and employed and that the appended claims are intended to be construed to include such variations except insofar as limited by the prior art.

25

**Claims**

- 1) A method to capture and validate a signature using a mobile device, the method comprising:
- 5           – the mobile device prompting a user to log into a user account located on a first server;
- the user signing on a touch sensitive screen of the mobile device;
- the mobile device capturing a signature of the user;
- 10          – the mobile device transmitting the captured signature to the first server to be validated.
- 2) A method as claimed in claim 1, further comprising:
- storing the validated captured signature on the first server.
- 15   3) A method as claimed in claims 1 or 2, further comprising:
- the mobile device retrieving, from the user account, at least one item to be signed;
- the mobile device displaying the at least one retrieved item;
- the user selecting at least one of the at least one retrieved item.
- 20   4) A method as claimed in claim 3, further comprising:
- associating the validated captured signature to the at least one of the at least one retrieved item.
- 25   5) A method as claimed in claims 1 or 2, further comprising:
- associating at least one item to be signed with the user account;
- the user receiving signing instructions.
- 30   6) A method as claimed in claim 5, wherein the signing instructions are received on the mobile device.
- 7) A method as claimed in claims 1 or 2, further comprising:
- creating at least one item to be signed;

- associating the at least one item with the user account;
- the user receiving signing instructions.

5 8) A method as claimed in claim 7, wherein the signing instructions are received on the mobile device.

9) A method as claimed in anyone of claims 5 to 8, further comprising:

- the mobile device retrieving, from the first server, the at least one item;
- the mobile device displaying the at least one retrieved item;
- 10 – the user selecting the at least one retrieved item.

10) A method as claimed in claim 9, further comprising:

- retrieving the validated captured signature from the first server.

15 11) A method as claimed in claims 9 or 10, further comprising:

- associating the validated captured signature to the at least one retrieved item.

12) A method as claimed in claim 11, further comprising:

- 20 – storing the associated validated captured signature on a second server.

13) A method as claimed in claim 1, further comprising:

- creating the user account on the first server, the user account having associated therewith at least one unique identifier.

25

14) A method as claimed in anyone of claims 1 to 13, further comprising:

- comparing the captured signature with previously captured signatures;
- determining whether the captured signature is forged;
- as a function of the determination, transmitting a validation
- 30 notification.

15) A system for the capture and validation of a signature, the system comprising:

a) at least one first server having stored therein at least one user account, the user account having associated therewith at least one item to be signed;

b) at least one mobile device comprising at least one touch sensitive screen, the at least one mobile device being capable of establishing communication with said at least one first server, of accessing the at least one user account, of retrieving the at least one item, of allowing a user to select the at least one item, of capturing a signature of the user with the at least one touch sensitive screen, and of transmitting the captured signature to the at least one first server for validation.

16) A system as claimed in claim 15, wherein the at least one first server is capable of storing the validated captured signature.

17) A system as claimed in claims 15 or 16, further comprising at least one second server capable of establishing communication with said at least one first server, of retrieving the validated captured signature from the at least one first server, and of associating the retrieved validated captured signature with the at least one item.

18) A system as claimed in claim 17, wherein the at least one second server is capable of storing the associated validated captured signature.

19) A method in accordance with the principles of the invention described hereinabove.

20) A system in accordance with the principles of the invention described hereinabove.

\* \* \*