

【DESCRIPTION】

【Invention Title】

MOBILE AUTHENTICATION METHOD AND SYSTEM THEREFOR

【Technical Field】

5 The present invention relates to a mobile authentication method and a system therefor, and more particularly, to an authentication method for performing self-verification and a financial transaction, such as a payment, using a phone number of a portable device extracted using a short message service (SMS) message of the portable device and unique user identifiers (UUID) of an application (app) installed
10 on the portable device and a system therefor.

【Background Art】

Due to the recent prevalence of smart phones, various financial transaction services, such as a payment or an account transaction, are being provided through smart phone apps. In addition to financial transaction services, various services
15 which require authentication are being used through smart phone apps.

In the case of a financial transaction, self-verification or authentication of a portable device is important. Therefore, authentication is frequently performed using a certificate, an automatic response system (ARS), an SMS, and the like. However, a financial transaction involves a troublesome procedure, such as inputting
20 a password of a certificate in every transaction or making a phone call to an ARS and inputting a temporary self-verification number, receiving an SMS message, and inputting a self-verification number included in the SMS message.

Since anyone can easily create and distribute smart phone apps, various apps are being created and used. While users can easily use all services, such as

financial transaction services, in smart phones, apps are highly likely to be tampered because anyone can create and distribute apps.

Also, when a smart phone is hacked and an app is copied or a smart phone is copied and used, personal information or financial transaction information may be
5 leaked.

【Disclosure】

【Technical Problem】

The present invention has been developed from the aforementioned technical background and is directed to providing a portable device authentication method for
10 preventing copying or misuse of an app by performing self-verification and app authentication with a self-verification number, which is generated on the basis of membership information including a phone number of a portable device, and UUID of the app and a system therefor.

The present invention is also directed to providing a method of extracting a
15 phone number of a portable device through an SMS server and using the extracted phone number for security when it is not possible to extract the phone number due to policy limitations and the like of a portable device manufacturer.

Objectives of the present invention are not limited to the aforementioned objectives, and other objectives which have not been mentioned will be clearly
20 understood by those of ordinary skill in the art from the following description.

【Technical Solution】

One aspect of the present invention provides a mobile authentication method including: extracting a phone number of a portable user device; transmitting membership information including the phone number to an authentication service

provider server for subscriber authentication; receiving a self-verification number from the authentication service provider server using the membership information; extracting UUID of an app installed on the portable user device and transmitting the extracted UUID of the app and the received self-verification number to a service
5 server; and receiving a serial number of the app, which is generated in correspondence with the self-verification number and the UUID of the app received by the service server, from the service server.

Another aspect of the present invention provides a mobile payment system including: a portable user device configured to receive a self-verification number by
10 transferring membership information including a phone number to an authentication service provider server and receive a serial number of an installed app by transferring UUID of the app and the self-verification number to a service server; the authentication service provider server configured to receive the membership information, performs membership authentication using the phone number included
15 in the membership information, and transmit the self-verification number to the portable user device after authentication; and the service server configured to generate the serial number of the app using the UUID of the app and the self-verification number received from the portable user device, store the generated serial number of the app, and transmit the generated serial number of the app to the
20 portable user device.

【Advantageous Effects】

According to the present invention, self-verification and authentication of a financial transaction app are performed together using membership information including a phone number of a portable user device and UUID of the financial
25 transaction app. Therefore, security of a mobile financial transaction can be

strengthened, and it is possible to prevent the financial transaction app from being copied and misused. Consequently, it is possible to prevent economic loss caused by leakage of financial information and the like.

In addition, even when it is not possible to extract a phone number of a portable device due to policy limitations and the like of the portable device manufacturer, the phone number can be extracted through an external device, such as an SMS server, and used for security.

【Description of Drawings】

FIG. 1 is a sequence diagram of an authentication method for a mobile financial transaction according to an embodiment of the present invention.

FIG. 2 is a sequence diagram of a phone number extraction method according to an embodiment of the present invention.

FIG. 3 is a sequence diagram of a method of checking authentication of a financial transaction app using UUID of the app according to an embodiment of the present invention.

FIG. 4 is a sequence diagram of a financial transaction method employing a financial transaction app which has been authenticated according to an embodiment of the present invention.

FIG. 5 is a structure diagram of a mobile payment system according to another embodiment of the present invention.

FIG. 6 is a structure diagram of a service server which performs authentication according to another embodiment of the present invention.

【Modes of the Invention】

Advantages and features of the present invention and methods for accomplishing the same will be more clearly understood from embodiments described in detail below with reference to the accompanying drawings. However, the present invention is not limited to the embodiments set forth herein but may be
5 implemented in various different forms. The embodiments are provided only to complete disclosure of the present invention and to fully convey the scope of the invention to those of ordinary skill in the technical field to which the present invention pertains, and the present invention is defined by only the scope of the claims. Meanwhile, terms used in this specification are for describing the
10 embodiments rather than limiting the present invention. In this specification, singular forms include plural forms unless expressly stated otherwise. As used herein, the word “comprises” and/or “comprising” do not preclude the presence or addition of one or more elements, steps, operations and/or devices other than stated elements, steps, operations and/or devices.

15 Hereinafter, exemplary embodiments of the present invention will be described in detail with reference to the accompanying drawings. For description convenience and improved understanding of each embodiment, a financial transaction app will be described as an example. However, the present invention is not limited to a financial transaction app and may be applied to various kinds of apps
20 which require authentication.

FIG. 1 is a sequence diagram of a self-verification method according to an embodiment of the present invention.

Self-verification of FIG. 1 corresponds to a user information registration step for authentication according to the present invention.

When a financial transaction app is downloaded and run for a financial transaction such as a payment or an account transaction (S110), a user agrees to clauses for financial transactions and input membership information, such as a user name and birthdate, local or foreigner, and male or female (S112).

5 Subsequently, a step for extracting a phone number of a portable device is performed (S120).

When an operating system (OS) of the portable device provides a phone number of the portable device like Android of Google, it is possible to simply extract the phone number from device information of the portable device through the OS.

10 However, when the OS does not provide device information, such as the phone number of the portable device, like iOS used in iPhones, it is possible to extract the phone number using an SMS.

After acquiring the phone number through the phone number extraction process (S120), the portable device acquires information of a communication service
15 provider through an input of the user's selection (S130) and transmits the phone number to a service server together with the already input membership information such as the name and birthdate (S132).

The service server requests authentication by transferring the received information to an authentication service provider server (S134). The membership
20 information including the phone number may be transmitted directly to the authentication service provider server not through the service server.

When the authentication service provider server requests subscriber checking by transmitting the received membership information including the phone number to the communication service provider server (S136), the communication service
25 provider server performs subscriber checking by comparing the membership

information including the phone number with subscriber information (S138) and notifies the authentication service provider server of the result (S140).

When subscriber checking is finished, the authentication service provider server notifies the service server that the authentication has succeeded by generating
5 and transmitting a self-verification number to the service server (S142), and the service server transfers the self-verification number to the portable terminal of the user (S144). The self-verification number may be transferred from the authentication service provider server directly to the portable terminal of the user not through the service server.

10 When self-verification is performed as described above, app authentication is performed in succession. The portable user device which receives the self-verification number is additionally subjected to checking of financial app authentication using the phone number and UUID of the financial transaction app (S150) so that a financial transaction service may proceed with strengthened security.

15 A method of extracting a phone number of a portable user device when a portable device OS restricts or does not support extraction of a phone number like iOS will be described in detail below, and app authentication using an extracted phone number and app UUID will be described in succession.

FIG. 2 is a sequence diagram of a phone number extraction method.

20 The portable device transmits an SMS message including a server authentication number (an index for the service server to check and manage the phone number of the portable device) generated by the financial transaction app to an SMS server (S1210).

When the SMS message transmitted from the portable device is received, the
25 SMS server extracts and acquires the server authentication number and the phone

number which is automatically included and transferred in the SMS message (S1220) and transmits the server authentication number and the phone number to the service server (S1230). The service server stores the received phone number of the portable device and the server authentication number together (S1240). In other
5 words, the phone number of the portable device and the server authentication number are stored in association with each other.

The SMS message passes through the SMS server, and in this process, the phone number of the portable device is automatically checked. Therefore, it is possible to prevent forgery of a phone number caused when a portable device
10 operator (e.g., a stealer) and the like inputs a phone number by mistake, and it is possible to detect a phone number even in a portable device, such as an iPhone, from which device information is not acquired.

The portable device requests the phone number by transmitting the server authentication number to the service server (S1250). The service server compares
15 the server authentication number received from the portable device with stored server authentication numbers and extracts a phone number corresponding to a server authentication number which coincides with the received server authentication number (S1260).

The service server transmit the phone number to the portable user device
20 using the extracted phone number (S1270) so that the phone number of the portable device may be prevented from being forged. Meanwhile, the portable device receiving the phone number may be configured to automatically display the received phone number therein so that the user may be notified that the phone number has been successfully extracted (S1280).

Meanwhile, step S1260 may be omitted, and when the service server acquires the phone number of the portable device in step S1240, the process may directly proceed to step S1280 so that the phone number may be transferred to the portable device.

5 The above-described process may be performed in a manner in which a portable device transmits an SMS message to a service provider, an SMS server transfers the SMS message transmitted by the portable device to a service server or another server managed by a service provider, and the service server or the other server extracts a phone number. In this case, no server authentication number may
10 be required.

According to such a phone number extraction method, unlike a conventional method in which a user personally inputs a phone number of a portable device and requests a self-verification number from an authentication service provider server, a phone number is automatically extracted by an SMS server so that forgery of the
15 phone number may be prevented.

FIG. 3 is a sequence diagram of a method of checking authentication of a financial transaction app using UUID of the app according to an embodiment of the present invention. When the user checks the self-verification number received by the portable device and inputs the self-verification number (S1510), the portable
20 device extracts UUID of the financial transaction app through the OS (S1520). Since the portable user device has received and stored the self-verification number already, it is obvious for those of ordinary skill in the art that a procedure for checking UUID of the app may be performed without an input of the user.

UUID are IDs which are given by an app storage, such as App Store, when an
25 app is downloaded from the app storage. Every time an individual downloads an

app, different UUID are given to the app, and the given UUID are stored not in the app but in an OS of a portable device to which the app has been downloaded. Therefore, even when the app is copied, the UUID are not copied. Consequently, it is possible to prevent tampering of the app.

5 When the UUID of the financial transaction app, the self-verification number, and the phone number of the portable terminal are transferred to the service server (S1530), the service server requests checking of the self-verification number by transferring the self-verification number and the phone number to the authentication service provider server (S1540).

10 The authentication service provider server authenticates whether the user (a person who has the portable device) coincides with the subscriber by comparing the self-verification number generated for phone number authentication and the phone number with the self-verification number and the phone number received from the service server in step S1540 (S1550). In other words, it is possible to check
15 whether the UUID are UUID transferred from the portable terminal which has requested generation of a self-verification number in steps S110 to S144 (possession authentication).

 The authentication service provider server notifies the service server of the authentication result (S1560), and the service server determines that the self-
20 verification has been finished and then registers membership information for providing a financial transaction service (S1570). The registered membership information includes the phone number of the portable device, the birthdate, local or foreigner, male or female, and the UUID of the financial transaction app.

 Meanwhile, when the self-verification is finished, the service server may
25 additionally generate an app serial number and store and manage the app serial

number together with the self-verification number, the app UUID, and/or the phone number of the portable device. After that, the service server may use the app serial number to check the authentication result. When self-verification and membership information registration are finished, the service server notifies the portable device of the user that a self-verification and registration procedure has been finished and also transfers the generated serial number of the financial transaction app (S1580) so that the serial number may be stored in the portable user device and then used for authentication when the financial transaction app is executed.

Meanwhile, it has been described above that the service server and the authentication service provider server are separate servers, but the service server and the authentication service provider server may be implemented as one server and maintained by one service provider. In this case, it is unnecessary to exchange data between the service server and the authentication service provider server.

After the above self-verification and authentication of the financial transaction app are finished, a financial transaction of the user is performed using the financial transaction app whose authentication has been finished. FIG. 4 is a sequence diagram showing a method of performing a financial transaction using a financial transaction app after authentication is finished.

When there is a payment request of the user, a franchise owner transmits the amount of payment, the phone number of the portable user device and the birthdate information of the user to the service server which provides a secured financial transaction through a franchise device (S410).

When the payment of the user is made online through the portable device, the amount of payment, the phone number and the birthdate information may be transmitted from the portable device of the user to the service server.

The service server determines whether the user is a member by comparing the phone number and the birthdate information received from the franchise device with the phone number and the birthdate in the membership information which has been stored in a database during a membership registration process (S420). When it is
5 determined that the user is a member, the service server extracts the previously stored serial number of the financial transaction app using the phone number (S430).

The service server requests the portable user device to execute the financial transaction app in a push manner using the user's phone number received from the franchise device (S440). In response to this, the portable user device executes the
10 financial transaction app (S450). A plurality of financial transaction apps may be installed on the portable device. In this case, it is possible to distinguish an app whose execution will be requested in a push manner using an app-specific identifier (app ID). Every time an app is installed on the portable device, the service server generates or acquires and stores an app ID and manages the app ID.

15 To prevent misuse of the portable user device such as theft or loss, a step of receiving a password or biometric information, such as a fingerprint or a signature, from a user may be added when the app is executed.

The executed financial transaction app extracts the UUID thereof through the OS, extracts the serial number thereof which has been received from the service
20 server and stored during a self-verification process (S460), and transfers the UUID and the serial number thereof to the service server to authenticate a financial transaction (S470).

The service server determines whether the app has been tampered by comparing the received UUID and app serial number with the UUID and the serial
25 number of the financial transaction app in the membership information which is

stored in the database when membership registration and self-verification are finished (S480).

Security may be further strengthened by using not only the aforementioned phone number and birthdate but also the serial number and the UUID of the financial transaction app for financial transaction authentication. The serial number or the UUID of the financial transaction app is not personally input by the user, but rather the serial number or the UUID stored in the portable device and the service server is used. Therefore, it is also possible to minimize the user's inconvenience caused by strengthened security.

When authentication of the financial transaction app is finished in this way, a financial transaction is possible in various ways in which a general payment service is provided (S490).

Meanwhile, the portable device may transfer only one of the app serial number and the app UUID to the service server, and the service server may determine whether the app has been tampered using the app UUID or the app serial number. However, when the app serial number and the app UUID are used together, it is possible to detect universal subscriber identity module (USIM) replacement, app dump, illegal app copying, etc. by analyzing the information together with a phone number, and thus security is further strengthened. Therefore, it is preferable to use the app serial number and the app UUID together.

FIG. 5 shows a system 50 for self-verification and financial transaction app authentication according to an exemplary embodiment of the present invention.

The system 50 includes a portable user device 510, an SMS server 520, a service server 530, an authentication service provider server 540, and a communication service provider server 550.

The portable user device 510 transfers a phone number and a server authentication number by transmitting an SMS message to the SMS server through the above-described process, receives the phone number from the service server 530 which receives the phone number and the server authentication number from the SMS server, and displays the received phone number on a screen.

In addition to the method employing an SMS, the portable user device 510 may use a method of directly extracting the phone number from an OS thereof.

According to the present invention, self-verification may be performed using the phone number received from the service server 530 or directly extracted from the portable user device 510 and a self-verification number received from the authentication service provider server 540, and a financial transaction app is authenticated by the service server 530 using an UUID and a serial number of the financial transaction app in order to determine whether the app installed on the portable device 510 has been tampered so that a financial transaction may be performed.

The SMS server 520 acquires the phone number of the portable device 510 from the SMS message received from the portable device 510 of a user and causes the phone number to be transferred to the portable device 510 by transferring the phone number to the service server 530, thereby serving to extract the phone number from the portable device 510, such as iPhones, in which access to the OS is restricted.

The service server 530 transfers the phone number to the portable user device 510 using the phone number and the server authentication number received from the SMS server 520, registers membership information of the user for a financial transaction service and generates and transfers a serial number of the financial

transaction app to the portable device 510 so that self-verification and authentication of the financial transaction app may be performed.

Also, when there is a payment request of a franchise terminal (not shown), the service server 530 causes the financial transaction app of the portable user device 510 to be executed in a push manner, receives the serial number and the UUID of the financial transaction app from the portable device 510, and determines whether the financial transaction app has been tampered by comparing the received serial number and the UUID with a serial number and UUID of the financial transaction app stored in a database so that a financial transaction process such as a payment may be performed.

The authentication service provider server 540 generates a self-verification number for self-verification. The authentication service provider server 540 requests subscriber checking from the communication service provider server 550 using the membership information which is received from the service server 530 and includes the phone number. When the communication service provider server 550 checks subscription information and notifies the authentication service provider server 540 of the result, the authentication service provider server 540 generates and transfers a self-verification number to the portable device 510 so that self-verification may be performed.

The communication service provider server 550 performs subscriber checking by comparing user information received from the authentication service provider server 540 with subscriber information stored in a database of the communication service provider server 550 and transfers the result to the authentication service provider server 540 so that self-verification may be performed.

Meanwhile, the service server may function as the SMS server 520 and the authentication service provider server 540.

Since the above-described system may prevent app tampering, a safe financial transaction is possible.

5 FIG. 6 is a structure diagram of the service server 530 which performs user authentication according to another embodiment of the present invention.

The service server 530 includes an authentication information transceiver unit 532, a membership information storage unit 534, and an authentication unit 536.

10 The authentication information transceiver unit 532 exchanges information required for user authentication with the portable user device 510 and the authentication service provider server 540.

First, the authentication information transceiver unit 532 receives membership information including a phone number from the portable user device 510 and transmits the received membership information to the authentication service provider server 540. The authentication information transceiver unit 532 receives a result of user checking, which is performed by the authentication service provider server 540 using the membership information, together with a self-verification number and transmits the result and the self-verification number to the portable user device 510.

20 The membership information storage unit 534 stores membership information required for authentication.

The membership information storage unit 534 stores the membership information including the phone number and received from the portable user device 510 and stores a self-verification number received from the authentication service provider server 540.

25

When user authentication succeeds with the self-verification number, UUID received from the portable user device 510 and an app serial number which is generated in correspondence with the UUID are stored in the membership information storage unit 534.

5 Finally, the authentication unit 536 performs user authentication by comparing the self-verification number received from the portable user device 510 and the self-verification number received and stored from the authentication service provider server 540.

Also, when an app serial number and/or UUID are received from the portable
10 user device 510 together with a payment request, the authentication unit 536 performs app authentication in which an app is verified by comparing the received app serial number and/or UUID with the app serial number and/or the UUID stored in the membership information storage unit 534, in a payment step.

By simultaneously using user authentication and app authentication, it is
15 possible to further strengthen security of a financial transaction in a mobile environment.

Although configurations of the present invention have been described in detail above with reference to the accompanying drawings, these are mere examples, and those of ordinary skill in the technical field to which the present invention
20 pertains can make various modifications and changes within the technical spirit of the present invention. For example, since it is possible to uniquely identify a specific app installed on a specific portable device with only UUID, the technical spirit of the present invention includes a configuration in which an app serial number is not used in user authentication and/or payment and a configuration in which any
25 password or biometric information instead of a birthdate is stored in a service server

and used for a payment. Therefore, the scope of the present invention should not be limited by the above-described embodiments but should be determined by the following claims.

【CLAIMS】

【Claim 1】

A mobile authentication and registration method performed in a portable user device, the method comprising:

receiving member information on a member's personal information other than the mobile phone number from a user;

extracting a phone number of the portable user device without user input;

transmitting membership information and the phone number to an authentication server;

receiving a self-verification number, which is a result of performing self-verification with the membership information, from the authentication server;

extracting unique user identifiers (UUID) of an application (app) installed on the portable user device;

transmitting the extracted UUID of the app, the extracted phone number, and the received self-verification number to a service server; and

receiving a self-verification number checking result, which is obtained by transmitting the self-verification number and the phone number received by the service server to the authentication server, from the service server.

【Claim 2】

The mobile authentication and registration method of claim 1, wherein the extracting of the phone number comprises:

transmitting a short message service (SMS) message including a server authentication number, which is generated by the app to authenticate the portable device, to an SMS server;

requesting the phone number of the portable user device by transmitting the server authentication number stored in the portable user device to the service server (which receives the phone number of the portable user device and the server authentication number from the SMS server and stores the received phone number and server authentication number); and
receiving the phone number from the service server.

【Claim 3】

A transaction authentication method performed by a service server after mobile authentication and registration of claim 1, the method comprising:

receiving a transaction approval request including membership information from a franchise device;

comparing the received membership information with stored membership information and transmitting an application (app) execution request to a portable user device corresponding to the membership information;

receiving unique user identifiers (UUID) of the app from the portable user device receiving the app execution request; and

comparing the received UUID with an app UUID included in the stored membership information and performing a payment when the received UUID coincides with the app UUID.

【Claim 4】

A mobile authentication system comprising:

a service server configured for the portable authentication, possession authentication, user authentication to receive automatically extracted phone numbers without user input and membership information about a member's personal information entered by the user directly into an app installed on the user's mobile device(excluding the mobile phone number) from a portable user device, request self-verification from an authentication server using a phone

number included in the membership information, receive a self-verification number as a result of the self-verification request, and transfer the self-verification number to the portable user device, and

configured for application (app) authentication of the app that can prevent illegal copying and forgery of the app to receive app unique user identifiers (UUID), a phone number, and the self-verification number from the portable user device, transfer the app UUID, the phone number, and the self-verification number to the authentication server together with the phone number, and, when authentication succeeds, performs membership registration and transfer a notification that self-verification has been finished to the portable user device; and

the authentication server configured for self-verification to perform subscriber checking by requesting subscription verification from a communication service provider according to the self-verification request of the service server, generate a self-verification number according to a result of the subscriber checking, store the self-verification number together with the phone number, and transmit the self-verification number to the service server, and configured for app authentication to compare the self-verification number and the phone number received from the service server with the stored self-verification number and phone number and transfer a result of checking app authentication to the service server.

【Claim 5】

The mobile authentication system of claim 4, further comprising a short message service (SMS) server configured to receive an SMS message including a server authentication number from the portable user device and transfer the server authentication number to the service server together with the phone number of the portable user device.

【Claim 6】

The mobile authentication system of claim 4, wherein the service server receives a payment request including the phone number of the portable user device from a franchise device, transmits an app execution request to the portable user device corresponding to the phone number, compares, when the app UUID is received from the portable device, the received app UUID with an app UUID corresponding to the stored membership information, and makes a payment when the received app UUID coincides with the app UUID.

【Claim 7】

A method of performing user authentication in a service server using a portable device of a user and an authentication server, the method comprising:

receiving membership information including a phone number from the portable device for the portable authentication, possession authentication, user authentication to receive automatically extracted phone numbers without user input and membership information about a member's personal information entered by the user directly into an app installed on the user's mobile device(excluding the mobile phone number) from a portable user device, request self-verification from an authentication server using a phone number included in the membership information, receive a self-verification number as a result of the self-verification request, and transfer the self-verification number to the portable user device,) transmitting a subscriber checking request to the authentication server together with the phone number;

receiving a self-verification number from the authentication server and transmitting the self-verification number to the portable device;

receiving unique user identifiers (UUID) of an app installed on the portable device, a phone number of the portable device, and the self-verification number from the portable device and transferring the UUID, the phone number, and the self-verification number to the

authentication server together with a self-verification checking request; and

transmitting an authentication check result received from the authentication server to the portable device.

【Claim 8】

An authentication service server comprising:

an authentication information transceiver unit configured to receive for the portable authentication, possession authentication, user authentication to receive automatically extracted phone numbers without user input and membership information about a member's personal information entered by the user directly into an app installed on the user's mobile device(excluding the mobile phone number) from a portable user device, receive a self-verification number as an authentication result based on the membership information from an authentication server by transmitting the membership information to the authentication server, transmit the received self-verification number to the portable device, and receive unique user identifiers (UUID) of an application (app) installed on the portable device, a phone number of the portable device, and a self-verification number stored in the portable device from the portable device;

a membership information storage unit configured to store the membership information including the phone number and received by the authentication information transceiver unit, the self-verification number, and the UUID; and

an authentication unit configured to perform authentication in a payment step by comparing an app UUID received together with a payment approval request from the portable device with the UUID stored in the membership information storage unit.

【Claim 9】

The authentication service server of claim 8, wherein the authentication unit performs app authentication by comparing the self-verification number received from the

portable user device with the self-verification number received and stored from the authentication server.