

CLAIMS:

1. A mobile device for enabling secure authentication between a user and a third party using a one-time-passcode (OTP) authentication mechanism, the mobile device comprising:

a mobile device screen for displaying information to the user; and

first circuitry configured to implement a local one-time-passcode generating module which is configured to:

generate at regular intervals a local one-time passcode which is unique to the mobile device and is valid for use in a single authentication, wherein the local one-time-passcode is a regularly changing local one-time-passcode;

receive, from second circuitry configured to implement a remote authentication module, a third party one-time passcode which is unique to the third party via a short message service (SMS) message sent from the remote authentication module; and

combine the regularly changing locally generated local one-time-passcode with the received third party one-time-passcode to generate a combined one-time-passcode for authenticating the user to the third party,

wherein the combined one-time-passcode is displayed to the user on the mobile device screen.

2. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to generate the combined one-time-passcode by generating a message which contains both the local and third party one-time-passcodes which are displayed to the user.

3. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to generate the combined one-time-passcode by cryptographically combining both the local and third party one-time-passcodes and displaying the cryptographically combined one-time-passcode to the user.

4. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to generate a local one-time-passcode for each third party of a plurality of third parties comprising the third party.

5. A mobile device according to claim 4, wherein the local one-time-passcode generating module is configured to determine from which third party the third party one-time-passcode was received and to select the local one-time-passcode associated with the determined third party.

5

6. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to:

extract the third party one-time-passcode from the received SMS message; and

10 combine the extracted third party one-time-passcode with the local one-time-passcode in a cryptographically secure manner.

7. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to generate a local one-time-passcode for each third party and wherein the local one-time-passcode generating module is configured to:

15 determine from which third party the SMS message was received; and

select the local one-time passcode associated with the determined third party.

8. A mobile device according to claim 7, wherein the local one-time-passcode generating module is configured to display the name of the determined third party with the local one-time-passcode associated with the determined third party together with the third party one-time passcode.

20

9. A mobile device according to claim 1, which is configured to receive the third party one-time-passcode via a first channel and wherein the mobile device is further configured to transmit, via a second channel, the combined one-time-passcode to the remote authentication module to authenticate the user to the third party.

25

10. A mobile device according to claim 1, wherein the local one-time-passcode generating module is configured to generate the local one-time-passcode using a time source.

30

11. A system for enabling secure authentication between a user and a third party using a one-time-passcode (OTP) authentication mechanism, the system comprising:

first circuitry configured to implement remote authentication module; and

35 a mobile device comprising:

a mobile device screen for displaying information to the user; and

second circuitry configured to implement a local one-time-passcode generating module which is configured to:

5 generate at regular intervals a local one-time-passcode which is unique to the mobile device and is valid for use in a single transaction, wherein the local one-time-passcode is a regularly changing local one-time-passcode;

receive, from the remote authentication module, a third party one-time-passcode which is unique to the received third party via a short message service (SMS) message sent from the remote authentication module; and

10 combine the regularly changing locally generated local one-time passcode with the received third party one-time-passcode to generate a combined one-time-passcode for authenticating the user to the third party, wherein the combined one-time-passcode is displayed to the user on the mobile device screen.

12. The system of claim 11, further comprising third circuitry configured to implement
15 a third party one-time-passcode generation module for generating a third party one-time-passcode which is unique to the third party.

13. The system of claim 12, further comprising a first channel through which the third
20 party one-time-passcode is sent from the third party one-time-passcode generation module to the mobile device and a second channel through which the combined one-time-passcode is sent to the authentication module.

14. The system of claim 11, wherein the local one-time-passcode generating module
25 is configured to generate the local one-time-passcode using a time source.

15. A method of using a mobile device to enable secure authentication between a
user and a third party using a one-time-passcode (OTP) authentication mechanism, the
method comprising:

30 generating at regular intervals, at the mobile device, a local one-time-passcode which is unique to the mobile device, wherein the local one-time-passcode is regularly changing local one-time-passcode;

receive, at the mobile device, a third party one-time-passcode from circuitry
implementing a remote authentication module, the third party one-time passcode
received via a short message service (SMS) message sent from the remote
35 authentication module, wherein the third party one-time-passcode is unique to the third party;

combining, at the mobile device, the regularly changing locally generated local one-time-passcode with the received third party one-time-passcode to generate a combined one-time-passcode for authenticating the user to the third party; and displaying, at the mobile device, the combined one-time-passcode.

5

16. A non-transitory computer-readable medium for enabling secure authentication between a user and a third party using a one-time-passcode (OTP) authentication mechanism, the non-transitory computer-readable medium storing instructions that, when executed by a hardware processor, cause the hardware processor to perform the method of:

10

generating at regular intervals, at the hardware processor, a local one-time-passcode which is unique to the hardware processor, wherein the local one-time-passcode is a regularly changing local one-time-passcode;

15

receive, at the hardware processor, a third party one-time-passcode from circuitry implementing a remote authentication module, the third party one-time-passcode received via a short message service (SMS) message sent from the remote authentication module, wherein the third party one-time-passcode is unique to the third party;

20

combining, at the hardware processor, the regularly changing locally generated local one-time-passcode with the received third party one-time-passcode to generate a combined one-time-passcode for authenticating the user to the third party; and displaying the combined one-time-passcode.