

CLAIMS:

1. A verification method comprising the step of:
using a software component installed on an electronic device to use an input to
5 generate, on the electronic device, at least one scrambled keypad configuration ;
generating, on the electronic device, an operable keypad and/or keypad image using
the at least one scrambled keypad configuration; and
presenting the keypad image over the operable keypad within a display zone of a
screen associated with the electronic device to generate a mapping between the
10 keys depicted in the keypad image and the keys of the operable keypad to allow an
encoded version of a user's identifier to be constructed.
2. A method according to claim 1 wherein:
the keypad image is an image of a non-scrambled keypad, and the operable keypad is
15 generated using the at least one scrambled keypad configuration.
3. A method according to claim 1 or 2 wherein:
the scrambled keypad configuration is generated on or at the electronic device by a
software component, preferably wherein the software component is:
20 installed on the electronic device after download from a remote resource.
4. A method according to claim 3 wherein the software component is arranged to generate
a Pin Entry Device.
- 25 5. A method according to any preceding claim wherein:
the operable keypad is one of a plurality of operable keypads, and/or the keypad image
is one of a plurality of keypad images, generated from the scrambled keypad
configuration.
- 30 6. A method according to claim 5 wherein:
the plurality of operable keypads and/or keypad images are arranged or ordered in a
series, stack, queue or other data structure.

7. A method according to claim 5 or 6 wherein one keypad in the plurality is designated or selected as the active operable keypad for receiving input from a user.
- 5 8. A method according to claims 5 to 7 and further comprising the step of:
re-ordering or otherwise altering the plurality of operable keypads after an input has
been received from a user.
9. A method according to claim 7 or 8 wherein:
 - 10 i) the selection or designation of the active operable keypad is changed such that
another operable keypad becomes selected or designated as the active operable
keypad; and/or
 - ii) the configuration of the keys on the operable keypad is altered to provide a different
ordering or arrangement of keys.
- 15 10. A method according to any preceding claim wherein:
the scrambled keypad configuration is generated using a true random number
generator or pseudo random number generator; or
the scrambled keypad configuration is generated using biometric data related to a
20 user.
11. A method according to any preceding claim wherein the electronic device is:
 - 25 i) a mobile and/or handheld device such as a smart phone, tablet, payment terminal
or smart-card reader; and/or
 - ii) a personal computing device associated with a user.
12. A method according to any preceding claim wherein the operable keypad and/or the
keypad image is erased from the device following input from a user, or following a
specified period of time.
- 30 13. A method according to any preceding claim wherein the position of the display zone
on the screen, and/or its dimensions, are specified by a procedure or method call,

preferably wherein the procedure call causes a keypad object to be created in volatile memory on the electronic device.

14. A method according to any preceding claim wherein the display zone comprises a plurality of sub-zones, each sub zone corresponding to a keypad key.
15. A method according to any preceding claim and further comprising the step of:
storing an encoded version of a user's identifier in memory associated with the electronic device, the identifier being received by the operable keypad via the keypad image such that the user's identifier is never stored on the device in an un-encoded form.
16. A method according to any preceding claim and further comprising the steps of:
storing the encoded version of the identifier entered into the electronic device by the operable keypad via the keypad image.
17. A method according to any preceding claim and further comprising the steps of:
transmitting the at least one scrambled keypad configuration and/or the encoded version of the user's identifier to a remote computing resource.
18. A method according to any preceding claim wherein different configurations are used to generate the image and the operable keypad so that the mapping is generated between the position of keys depicted in the image and keys of the operable keypad, and the encoded version of a user's input is created due to the mapping.
19. A method according to any preceding claim wherein the at least one scrambled keypad configuration specifies the order, arrangement or position of keys in the operable keypad or keypad image.
20. An electronic computing apparatus comprising a screen and at least one software and/or hardware component arranged and configured to perform the method of any preceding claim.

21. The device of claim 20 wherein the apparatus comprises or is associated with:
a true random number generator and/or a pseudo random number generator;
means for capturing or generating biometric data related to a user; and/or
5 means for reading data from a smart card.
22. A verification method comprising the steps of:
displaying a keypad image over a first operable keypad within a zone of a screen
associated with an electronic device;
10 using the first operable keypad to obtain a first keystroke from a user; and
using at least one further keypad to obtain at least one further keystroke;
wherein the configuration of the first and/or least one further operable keypad, and/or
the configuration of the keypad image, is determined using an input sequence
generated on or captured locally to the electronic device.