

Authentication Methods and Systems

This invention relates generally to the field of user authentication. The invention is suited for use in situations where a user is required to enter an identifier or code (eg a PIN,

5 password etc) which is validated prior to completing an operation. The operation might be any type of operation. The invention is also suited for, but not limited to, verification of the user on a mobile device such as a smartphone or tablet computer.

10 Authentication techniques are used in a variety of situations where an individual's identity and/or authorisation needs to be verified prior to being allowed to perform an act or gain access to some controlled or managed resource such as a device, building, a computer system, a financial account, a service etc..

One common approach to authentication is to record some pre-selected identifier
15 comprising a code or combination of symbols which is then maintained in secrecy in a secure location and available only to authorised parties. For the sake of convenience, the identifier may be referred to in this document as a Personal Identification Code (PIC) although it is important to note that the identifier may comprise other types and combinations of symbols and not just numeric digits. The term 'PIC' as used herein
20 should not be construed as limiting the invention with respect to the type or format of the user's identifier.

After the identifier has been selected and assigned to an authorised individual (or group of individuals), the user is required to supply the correct identifier each time he requests
25 permission to perform the controlled act or gain access to the resource or service. The user's inputted identifier is compared with the pre-stored version. If the input matches the stored identifier then the user's identity is deemed to have been verified and access is granted. Alternatively, if the input does not match the pre-stored version then access is denied.

30

The use of PINs has become commonplace, especially in relation to banking and financial applications. Customers have become accustomed to, and trusting of, the use of PIN-based

verification. Financial institutions also favour PIN-based authentication as it provides a more secure form of verification than, for example, a signature. Further still, when a transaction requires authentication via a PIN the liability for any fraud resulting from that transaction is deemed to lie with the user who has supplied the PIN. This is in contrast to
5 'card not present' transactions such as on-line transactions where the liability remains with the issuing financial institution.

Another authentication approach involves using a device to capture biometric data relating to the unique physical or behavioural attributes of the individual such as iris pattern, palm
10 geometry or fingerprint. An advantage of biometric authentication is that users do not need to remember passwords or codes, and the required information is always carried inherently by the individual wherever they go so no additional hardware such as tokens need to be carried. Therefore, biometric authentication offers a convenient and simple authentication solution which is attractive to end users.

15 However, despite the attractions of biometric authentication, it has yet to be widely adopted within certain industries such as the banking industry. One reason for this is that the infrastructure of the banking industry is geared towards verification using a 4 digit PIN. This includes payment terminals, ATMs, switches, and the apparatus at both the acquiring
20 and issuing banks, which would all need to be replaced or adapted at significant cost in order to move from PIN-based to biometric authentication. Other concerns arise in relation to the security of biometric data which may be captured from non-secure sources. For example, fingerprints can be 'lifted' from public places, voices can be recorded. In addition, while it is easy to change a stored PIN or identifier it is not possible for an
25 individual change biometric data such as fingerprint, iris pattern etc.

These concerns can be reduced by the use of two or three-factor authentication wherein at least two of the following are used during authentication:

- What you know (eg PIN, password)
- 30 • Who you are (eg fingerprint, retina pattern, face or voice patterns)
- What you have (eg smart card, security token, mobile device)

Therefore, a system which requires a user to authenticate with both a PIN and biometric data on a device owned or operated by the user would provide enhanced security.

With respect to mobile technology, more and more people are using handheld computing devices such as smart phones and tablet computers etc for identity-sensitive operations such as banking. However, such devices are notoriously insecure and passwords, PINs and other valuable authentication data can be compromised by third parties. Therefore, there is a significant challenge in providing an authentication solution which is secure even when used on a mobile device.

One such solution has been disclosed in WO 2014/013252 which teaches the concept of sending an image of a scrambled keypad from a server to a user's device (PC, mobile phone, tablet etc). An operable, functional keypad is generated on the device and the image is displayed on the screen in the same position as the keypad. The image is superimposed over the keypad such that it is hidden from view yet still functional in the background. The positions of the underlying keypad keys do not correspond to the positions of the same 'keys' depicted in the image. To the user, only the image of the scrambled keypad is visible and thus when the user touches or clicks on part of the image to select an input, the operable keypad interprets this input differently and an encoded version of the user's input is received into memory on the device. Thus, as the user's real identifier (eg PIN) is never entered into the keyboard buffer or elsewhere on the device it cannot be fraudulently obtained from it. The encoded identifier is then transmitted to a remote server which knows the order of keys depicted in the keypad image, and can thus decode the user's input. In effect, a mapping is created between the keypad configurations, and this mapping is used to both encode and decode the identifier. This solution provides significant advantages over other authentication techniques, because it does not require the user to remember a different identifier, does not require the use of special or additional hardware, and avoids entry of the user's real identifier into an insecure device.

EP 1615181 A1 discloses an authentication method wherein a random string is fed into an 'image generator' component. The image generator takes the random string and generates image data suitable for display on a client terminal. The image data is then used to change

the appearance of the display on the terminal so as to present the user with a plurality of characters and the user then inputs his PIN by selecting characters. Each input selected by the user is recorded as positional data by the client terminal (e.g. first row, second column). This positional data is then converted by the client terminal into character data eg the

5 numeral 2. In contrast to the WO 2014/013252 arrangement, there is no use of an operable keypad, masked by an overlying image, to perform the encoding during entry. Instead, a customised algorithm is used to post-process the positional data into an encoded version of the user's input.

10 An alternative solution has now been devised.

Thus, in accordance with the present invention there is provided an authentication solution as defined in the appended claims.

15 The invention may provide a verification method. It may be used to verify or authenticate the identity of a user prior to granting access to a controlled resource. The controlled resource may be a physical resource or a virtual, electronic or digital resource. The invention may provide an enhanced security solution.

20 The invention may comprise the step of:

generating an operable, scrambled keypad and providing said keypad within a display zone of a screen associated with an electronic device;

presenting an image of a non-scrambled keypad within at least part of the display zone such that at a user is able to operate at least one operable key of the keypad via (ie

25 through) the image.

Thus, the image and the keypad may be provided within the same display zone of the same screen. The user may enter or input an identifier by "selecting" a portion of the image.

This may cause an encoded version of the user's identifier to be generated and entered into

30 the device by the operable keypad. Thus, no post-entry transformation or processing of the identifier or its positional data is required in order to encode or translate it.

-5-

Preferably, the operable, scrambled keypad is generated at run-time (during use) by invoking a portion of code. The operable, scrambled keypad may be generated by a subroutine which is provided as standard with the device. The image may depict a keypad which is a default keypad associated with the device. The operable keypad may be or
5 comprise an event handler (or “event listener” in some alternative programming terminologies). The event may be a keyboard event, a touchscreen event or some other input-related event.

The image may be generated on the device, or may be received by the device from a
10 remote computing resource. The remote computing resource may be a server.

The operable keypad may be generated using a keypad configuration derived using a random, or pseudo-random, number, or biometric data relating to the user. The order of the operable keys in the operable keypad may be at least partially determined using
15 biometric data derived from or associated with the user. Preferably, the biometric data may comprise, or be processed to provide, one or more strings, arrays or sequences of values which can be used to specify the order of the operable keys.

In this document, the phrase “biometric data” may be used to mean data which is captured
20 directly from the user (i.e. “raw” biometric data such as may be captured by a sensor). It may also mean biometric data which has been derived from a biometric capture process. For example, it may be processed data which has been obtained or derived following a biometric authentication process.

25 A plurality of operable keypads may be generated. At least one keypad in the plurality may be a scrambled keypad. A plurality of keypad images may be generated. At least one image in the plurality may be an image of a non-scrambled scrambled keypad.

A mapping may be generated between keys depicted in the image of the non-scrambled
30 keypad and the keys of the operable keypad. The mapping may enable an encoded version of an input, from the user, to be inputted into the device. The method may comprise the step of transmitting the encoded version of the input to a remote computing resource.

The electronic device may be any device having a processor and computing capabilities. It may be a handheld computing device. It may be a mobile phone, a tablet computer, a payment terminal, a laptop, a portable computing device or a personal computer.

5

Also according to the invention there is provided a system arranged and configured to implement any embodiment of the method described herein. Any feature(s) described in relation to the method may also be applicable to the system, and vice versa.

10 Thus there is provided a verification system comprising:

an electronic device;

a screen associated with the electronic device;

wherein the electronic device is arranged to:

generate an operable, scrambled keypad and provide said keypad within a display zone

15 of the screen; and

present an image of a non-scrambled keypad within at least part of the display zone such that at a user is able to operate at least one operable key of the keypad via the image.

20 In one or more embodiments, the invention may comprise an apparatus or method substantially or partially as disclosed in WO 2014/013252. However, WO 2014/013252 discloses an arrangement wherein a plurality of scrambled keypad configurations is sent from a remote server to the electronic device for use in generating a plurality of scrambled, operable keypads. Moreover, WO 2014/013252 discloses the use of a scrambled image
25 superimposed over an operable keypad.

By contrast, in accordance with the present invention, the keypad image depicts a non-scrambled keypad. More than one image may be generated and used on top of one or more scrambled keypads. While one or more images in the plurality of images may depict a
30 scrambled keypad, at least one image in the plurality depicts a non-scrambled keypad. The use of a non-scrambled image superimposed or displayed over an operable keypad provides the advantage that the user is presented with a keypad configuration that is

-7-

familiar and expected. This results in fewer input errors being made by the user than when an image of a scrambled keypad is used.

As the image is not scrambled, the mapping between the non-scrambled image and the
5 scrambled operable keypad may need to be known by, or communicated to, the remote device (server) in order for decoding to be performed. Therefore, the use of a non-scrambled image gives rise to several non-trivial issues which must be addressed by the present invention.

10 A plurality of keypad images may be generated and/or a plurality of operable keypads. However, at least one of the images will depict a non-scrambled keypad and be provided over a scrambled, operable keypad so as to provide a mapping between the 'keys' of the image and the functional keys of the underlying operable keypad.

15 The term 'non-scrambled' in this context can be interpreted as meaning that the keys depicted in the image are in accordance with a standard format or configuration. The order of the 'keys' depicted in the image may be as expected by the user. The values assigned to the respective keys may therefore be contiguous. They may be arranged in ascending or descending order.

20

By contrast, the term 'scrambled' may be interpreted as meaning that the order of the keys is randomised, or somehow deviates from the default, standard or expected order. The standard configuration may be standard relative to the device. The term 'scrambled' may be used to mean that the keys in a keypad configuration are altered relative to a reference
25 configuration. The reference configuration may be specified by a keypad configuration which is native to, or provided as standard with, the device.

The image may be generated on the user's electronic device, or may be sent to and received by the device from a separate resource.

30

One or more keypad configurations may be sent to the device from a remote computing resource eg server. The one or more keypad configurations may be used to generate the

operable, scrambled keypad. The keypad configuration may be sent to the device as a filename.

Additionally or alternatively, one or more scrambled keypad configurations may be generated on or at the electronic device itself. The at least one scrambled keypad configuration may then be used to generate at least one operable keypad. The keypad image and/or operable keypad may also be generated on or at the electronic device. Advantageously, the workload is transferred from the remote resource to the local device. It also avoids the need for transmittal of the configuration(s) to the device.

10

The operable keypad may be generated by executing a subroutine such as a function, method or procedure on the electronic device. The subroutine may be part of a library. The library may be provided as standard to the electronic device. Execution of the subroutine may cause a keypad object to be generated in volatile memory on the electronic device. The keypad object may be a virtual, electronic model a mechanical keypad. The operable keypad may be generated at run-time.

15

The phrase 'on or at' may be interpreted as meaning that the scrambled keypad configuration is generated by the electronic device itself, or by one or more devices which are associated with the electronic device eg by physical or wireless connection to the electronic device. The scrambled keypad configuration may therefore be generated locally to the electronic device (client) rather than being received from a remote resource (server).

20

The phrase 'keypad configuration' may be used herein to refer to the order, arrangement or position of keys in a keypad. It may also be used to refer to the order of 'keys' as depicted in the keypad image although it should be noted that in reality the image does not actually comprise operable 'keys'.

25

Preferably, the scrambled keypad configuration is generated on or at the electronic device by a software component, which may be referred to as a keypad generation component (KGC), and may be arranged to generate the image(s) and/or operable keypad(s). Additionally or alternatively, it may be arranged to generate one or more configurations for

30

specifying the arrangement of keys in the scrambled operable keypad(s). . The keypad generation component may be arranged to generate a Pin Entry Device (PED). This may be a virtual, non-physical PED. The component may be installed on the electronic device after download from a remote resource ie remote with respect to the electronic device. The
5 remote resource may be a server. It may be a cloud-based resource.

The software component may be configured to receive an input. It may be configured to use the input to provide one or more keypad configurations for use in generation of the keypad image(s) and/or operable keypad(s). The input may be a pseudo or true random
10 number, or it may be biometric data related to a user. The user may or may not be associated with the electronic device.

The keypad image may be a representation of a keypad. It may be a static image or a moving image. It may comprise a watermark. It is distinct and distinguishable from the operable keypad in that the image resembles a keypad but does not comprise any keypad
15 functionality. Therefore, while portions of the image may represent or depict 'keys', and may appear as such to the user, the image itself or portions thereof do not possess any operable properties. Thus, clicking on, touching or otherwise selecting a portion of the keypad image may not, in itself, result in an input being received by the electronic device.
20 In one or more embodiments, one or more keys depicted in the image may be colour coded, watermarked or otherwise tagged to provide a visual assurance to the user that the image has been provided by a legitimate source.

By contrast, the operable keypad comprises the functionality and properties which the
25 skilled person would associate with a functioning keypad. Thus, the operable keypad may comprise a plurality of keys or buttons. The keypad is configured such that each key or button has a value (eg digit, letter or other symbol) associated with it. This assignment of values to keys may typically be performed upon creation of the keypad (when a subroutine is invoked at run time) but the associations may be changed after creation if the keypad is
30 re-configurable. In either event, the association of values to keys is performed prior to entry of the user's input such that when the user selects a given key, its pre-defined value is

put into a portion of memory in the electronic device. The portion of memory may be a keyboard buffer.

The invention may enable the user to provide an input to the electronic device by operating one or more keys of the operable keypad via or through the image. The keypad image may be superimposed over the operable keypad in the sense that the operable keypad is provided within the display zone of the screen but the image is presented at least partially within the same display zone such that it obscures or masks the operable keypad from the user's view. The operable keypad may be in the background, listening for an input, even though the user cannot see it. Preferably, the image masks the operable keypad completely so the user appears to see an operable keypad but in reality is only able to see an image of a keypad. Preferably, the symbols on the operable keys of the underlying keypad may not correspond to the position of the 'keys' as shown in the keypad image. This is because the image depicts a non-scrambled keypad while the underlying keypad is scrambled. In other words, the configuration of the operable keypad may not match or be the same as the configuration of the keypad depicted in the image. Thus, when the user selects what appears to be a key in the keypad image, the operable keypad active and listening within the display zone may cause a different symbol to be entered into the device's memory. In this manner, the user's real (ie intended) input may never be received into any portion of the device's memory. It may never be received by the keyboard buffer. An encoded version of the identifier is created due to the mapping between the different configurations used to generate the keypad and the image.

This feature provides the significant advantage that the user's real input cannot be obtained by any party who has gained unauthorised access to the electronic device. It also distinguishes the invention over known solutions wherein data such as positional data or an identifier is received from the user into memory and then translated into an encoded version of the user's input.

One or a plurality of operable keypads may be generated on the electronic device during an authentication session. Additionally or alternatively, one or a plurality of keypad images

may be generated during the session. One or more keypads may be generated from one (scrambled) keypad configuration.

A plurality of operable keypads and/or keypad images may generated. They may be
5 arranged or ordered in a series, stack or queue or other data structure.

One keypad in the plurality may be designated or selected as the active operable keypad for receiving input from a user. The active operable keypad may be the keypad which is provided 'beneath' the image such that when the user selects a portion of the image on the
10 screen, the active operable keypad is caused to function. Preferably, there is only one active keypad at any given point in time. The remaining operable keypads in the plurality may be dormant or inactive until designated as the active keypad. Thus, a plurality of operable keypads may be generated and placed into a data structure. The data structure may be iterated over so that the operable keypad designated as the active one changes over
15 time. The change may be effected following a certain period of time or after an event such as an input being received from a user. Thus, after an input from the user, the active operable keypad may be replaced or exchanged for another operable keypad in the plurality. The previously active keypad may be erased from memory, or marked for removal, once it has become inactive. Thus, once an input (keystroke) has been received
20 using a particular operable keypad it may be deleted from the electronic device.

Alternatively, rather than cycling through a plurality of pre-generated operable keypads, a new operable keypad may be generated for each input when needed. Each newly generated operable keypad may comprise a different configuration of keys from the others.
25 A new operable keypad may be generated when an input is expected or required from the user. For example, if the identifier is four digits long a first keypad may be used for receipt of the first input, then second keypad generated for receipt of the second input and so on for all four inputs.

30 Further still, a mutable (changeable) keypad may be provided in addition to or instead of a plurality of operable keypads. The configuration of the mutable operable keypad may be altered after or upon an event such as receipt of an input from a user, or after a certain

period of time. Thus, the same operable keypad may remain as the active one, but the arrangement of the keys may change. The scrambled keypad configurations may be used to determine the different configurations of the keypad.

- 5 The scrambled keypad configuration(s) may be generated using a true random number generator or pseudo random number generator. The true or pseudo random number (hereinafter simply 'the random number') may be fed as input into the software component referred to as the keypad generation component. Thus, when using a random number as input to the configuration component, different keypad configuration(s) may be produced
10 each time the invention is used by the same user.

Preferably, the random number is generated locally to the electronic device. It may be generated on the processor of the electronic device or using a device which is in local communication (wired or wireless) with the device. Thus, it may be generated by a plug-in
15 device or a device connected to the electronic device via a wireless protocol such as Bluetooth, NFC etc.

The scrambled keypad configuration may be generated using biometric data related to a user. The biometric data may be generated or captured in a variety of ways. As with
20 respect to the random number generation above, it is preferably generated by the electronic device or locally to the electronic device. The biometric data may comprise any form of data relating to a physical or behavioural attribute of the user. It may comprise data relating to, or derived from, a fingerprint, iris pattern etc. The biometric data may be derived from "raw" biometric data which has been captured by a biometric data capture
25 device. The invention is not to be limited with respect to the type of biometric data used or the manner in which it is collected or processed. Various biometric data capture and analysis systems are known in the art and considered to be suitable for use with the present invention.

- 30 The biometric data may be processed to provide a sequence or identifier which is unique to the user. The sequence may be a string of values or characters. This string may be fed into the software component (KGC) so as to specify the order of keys in one or more operable

keypads and/or images generated by or at the electronic device. Thus, when using biometric data as input to the software component, the same keypad configuration(s) may be produced each time the invention is used by the same user.

- 5 The biometric data may be used to generate a seed which is then used to influence the configuration(s). Additionally or alternatively, some other form of data may be used as the input to the keypad configuration algorithm. This data may be derived from or in some way related to the user's biometric data. It may be, for example, a cryptographic key. The cryptographic key may be used in the generation of a seed for input to the configuration
- 10 generation component. The key may be a private or public cryptographic key which is associated with the user and/or a digital wallet associated with the user. The wallet may be stored on the electronic device. The cryptographic key may have been generated during a biometric authentication process, or a registration process involving the capture of the user's biometric data. For example, the public/private key may have been generated during
- 15 the creation, set up or registration of a digital wallet such as, for example, a Bitcoin or other cryptocurrency wallet.

- The electronic device may be a mobile and/or handheld device such as a smart phone, tablet, payment terminal, payment card reader or smart-card reader. Additionally or
- 20 alternatively, it may be a personal computing device associated and/or registered with a user. This distinguishes the invention over those prior art arrangements which are designed for use with non-personal computing devices such as ATM machines. The term 'personal computing device' is used herein to refer to an electronic computing device, such as a PC, laptop, mobile phone, tablet computer which can be associated with, registered to,
- 25 and/or owned by an individual.

- Preferably, the operable keypad and/or the keypad image is erased from the device following one or more input(s) from a user, or following a specified period of time. The position of the display zone on the screen, and/or its dimensions, may be specified by a
- 30 subroutine such as a procedure or method call. The display zone may comprise a plurality of sub-zones, each sub zone corresponding to a keypad key. The sub-zone may be referred to as 'hot spots'. Thus, selection of a particular hot spot on the screen may cause a key of

-14-

the active, operable keypad to be activated such that an (encoded) input is placed into memory.

Preferably, the method comprises the step of storing an encoded version of a user's
5 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.

It may comprise the steps of storing an encoded version of an identifier entered into the
10 electronic device by the operable keypad via the keypad image; and transmitting the encoded version of the identifier to a remote computing resource.

A scrambled keypad configuration may be transmitted to the remote computing resource. A plurality of scrambled keypad configurations may be sent to the remote computing
15 resource. The remote computing resource eg server may decode the encoded version of the user's identifier. It may use one or more scrambled keypad configurations to decode the encoded version of the user's identifier.

The invention may be arranged to generate one keypad configuration for each value in the
20 user's identifier. Additionally, it may generate a keypad configuration for use in generating a keypad image.

The invention also provides an electronic computing apparatus arranged and configured to implement the method described above. The apparatus may comprise a screen and at least
25 one software component arranged and configured to perform any version of the method described above. The screen may be a touch screen.

The apparatus may comprise, or be associated with or in communication with:
a true random number generator and/or a pseudo random number generator;
30 means for capturing or generating biometric data related to a user; and/or

-15-

means for reading data from a smart card. The smart card may be a payment card. It may be any type of IC card which is independent of the operation of the device ie it may not be a SIM card.

- 5 The invention also provides a verification method comprising the steps of:
using biometric data related to an individual to generate a keypad configuration;
using the keypad configuration to generate an operable keypad and/or a keypad image.
Any or all of the features described above may also apply to this aspect of the invention. A plurality keypad images may be generated wherein at least one is an image of a non-
10 scrambled keypad.

Preferably, the keypad configuration is a scrambled keypad configuration. Thus, the order of keypad keys specified by the configuration may be altered relative to a default or reference configuration.

15

The method may include the steps of:
capturing, generating or receiving the biometric data on or at an electronic device;
generating the operable keypad and/or keypad image on or at the electronic device.

- 20 The invention also provides an electronic payment device comprising:
a touch screen;
a component arranged to read a payment card or other IC card; and
software arranged to:
generate at least one keypad configuration from biometric data related to
25 an individual, and/or a true or pseudo random number; and
generate a keypad image and/or operable keypad using the at least one keypad configuration.

- The payment or other IC card may be separate to the electronic device. It may be
30 physically independent of the electronic device. It may be a financial card such as bank or credit card. It may not provide functionality for the device. It may be distinct and different from a SIM card.

Also in accordance with the invention there is provided a verification method comprising the steps of:

5 displaying an image of a non scrambled keypad over a first operable keypad within a zone of a screen associated with an electronic device;
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 at least one further operable keypad,
and/or the configuration of the keypad image, is determined using an input sequence
10 generated on or captured locally to the electronic device.

Any or all of the features described above may also apply to this aspect of the invention.

The non scrambled image may be superimposed over the scrambled, operable keypad as
15 described above in relation to other aspects of the invention. In this way, the image may provide a mask or cover which obscures the operable keypad at least in part. Thus, the user may see the non scrambled keypad image instead of the scrambled operable keypad such that when the user selects a portion of the image, the operable keypad is caused to function. Thus, the method enables an encoded version of the user's input to be received by memory
20 (eg keyboard buffer).

A plurality of operable keypads may be generated on the electronic device. At any given time, one operable keypad may be selected or arranged as the active keypad. The active keypad may be the one which is executed by the device so as to obtain the next keystroke
25 from the user.

The input sequence may be a pseudo random number. Additionally or alternatively, the input sequence may be generated using biometric data related to the user.

30 An encoded version of an identifier may be constructed. The encoded identifier may comprise the first keystroke. It may comprise the at least one further keystroke. The

identifier may be a code, password or other any other type of identifier associated with the user.

The scrambled keypad may comprise a configuration of keys which are in a randomised order or a different order relative to a default or reference keypad configuration. A different scrambled, operable keypad may be used to obtain each keystroke obtained from the user. Each operable keypad in the plurality may be different from the others in the plurality in the sense that it is a separate, distinct operable keypad. Alternatively, only one mutable, operable keypad may be generated and the order of keys reconfigured for each keystroke. Thus, the keypads may be different in the sense of having different key configurations.

The electronic device may be a mobile or handheld device such as a smart phone, laptop computer, tablet computer or payment terminal. The electronic device may comprise software and/or hardware capabilities for reading data from a card. The card may be an IC or smart card such as a payment card. The card may be independent to the operation of the electronic device. In other words, the card may not be a SIM card or other 'card' integral to the operation of the device.

One or more aspects of the invention may be described as providing a two-factor authentication solution. It may provide a solution wherein:

- 1) The identity of the user is verified using biometric data; and
- 2) The user's authorisation to perform the transaction is verified by entry of a correct, pre-selected identifier.

25

It is important to note that for the sake of brevity and clarity, some features described above in relation to one aspect of the invention may not have been repeated in relation to other aspects of the invention. However, any feature mentioned above in relation to one aspect of the invention may be equally applicable to any other aspect of the invention.

Features described in relation to the system may also be used in relation to the method and vice versa.

30

These and other aspects of the present invention will be apparent from and elucidated with reference to, the embodiment described herein. An embodiment of the present invention will now be described, by way of example only, and with reference to the accompany drawings, in which:

5

Figure 1 shows a flowchart illustrating one possible embodiment in accordance with the method of the invention.

10 The invention provides a secure authentication solution for verifying the identity of an individual. The invention may be used as part of a wider authentication process or system not described herein.

In one embodiment, the present invention deviates from the authentication technique described in WO 2014/013252 which involves presenting an image of a scrambled keypad on a user's electronic device eg mobile phone such that it obscures an operable keypad from the user's view. The user, therefore, sees what appears to be an operable keypad, but in fact is simply an image devoid of functionality. In accordance with the present invention, however, at least one non-scrambled image is used in conjunction with a scrambled, operable keypad.

20

The operable keypad underlying the image comprises keys or buttons which have symbols assigned to them, as is known in the art. The operable keypad may be referred to as a virtual keypad. The user enters his/her identifier eg PIN, password, or personal identification code (PIC) by selecting portions of the screen which depict 'keys' corresponding to the symbols in the identifier. The operable keypad which has been generated behind the image detects the user's key strokes and enters the symbols assigned to the keypad's selected keys into the buffer. This allows an encoded version of the real identifier to be constructed and sent to a remote server for verification. It is important to note that the invention does not perform a translation or encoding operation on the user's input as is known in some prior art arrangements. In such known systems, the 'real' identifier is entered into the keyboard buffer before being encoded. This enables unauthorised parties to access the user's identifier via the buffer. The invention, however,

30

avoids this problem by never storing the real version of the identifier, even temporarily in the buffer.

As the order of the keys in the operable keypad is different from the order of the keys depicted in the image, the user's 'real' input is never actually entered into memory on the phone. This provides the significant benefit that the real identifier cannot, therefore, be derived by an unauthorised party from the phone. Further still, unless someone knows the configuration of keys in both the operable keypad and the keypad image, they cannot decode the encoded identifier.

10

In one embodiment, the keypad image and/or the configuration of keys for the operable keypad are generated on the user's device. This provides the advantage that the processing work is transferred to the client (user's) device rather than server. Alternatively, the image and/or configuration is being sent to the device from a remote server. In yet other embodiments, a mixture of on-device generation and server provided images/configurations may be used.

15

In one embodiment, a software component installed on the user's device receives an input. It uses that input to determine the configuration of keys for one or more operable keypads. Additionally or alternatively, it uses the input to determine the configuration of 'keys' to be depicted in one or more keypad images. The operable keypad(s) and/or keypad image(s) can then be generated using the configurations specified by the software component. However, at least one non-scrambled keypad image is used.

20

In one embodiment, the input to the generation component is a random number. In another embodiment, the input is biometric data relating to the user. The biometric data can be a fingerprint, for example. The skilled person will readily understand that any type of biometric data can be used. The invention is not limited with respect to the format, type or method of capture of the biometric data.

25

30

If a random number is used as input, the resulting configuration(s) will be different each time the invention is used. If, however, biometric data is used as the input, the resulting

-20-

configurations will be the same each time the invention is used. This is because the user's biometric data eg fingerprint, retina pattern etc remains constant and will always provide the same input.

5 In either embodiment, the input is generated on, by or at the user's device. In other words, it is generated locally to the user's device rather than by a remote resource. The input may be generated by one or more components which comprise part of the user's device, or are in proximity to the user's device and connected thereto by a physical or wireless interface.

10 In use, the user registers with a system in accordance with the invention. The requisite software is then downloaded to the user's device, including the generation component. Hereinafter, the user's device will be referred to as a mobile phone but any electronic device with computing capabilities may be used.

15 When the user's identity needs to be verified, the required input is generated either by a random number generator or by a biometric capture device. For example, the user may press a finger against the screen of the phone, or may look into a camera, or speak into a microphone etc. The biometric capture device generates a string which represents the captured biometric property.

20

The biometric data or random number (string) is then fed into the keypad generation component. This component then uses that input to generate a plurality of keypad configurations. Preferably, the order of symbols or values in each of the configurations is unique such that no configuration is duplicated. The keypad configurations may be
25 generated from the random or biometric string using values or substrings selected from the string. For example, the first ten values of the string may be used for the first 10-digit keypad configuration, the next ten values may be used for the second configuration and so on. Thus, the component must ensure that the input string is of sufficient length to provide the required values for the keypad configurations.

30

In an illustrative embodiment using a keypad comprising the digits '0' through to '9', there will be ten values (ie characters, digits or symbols) in each configuration generated by the

invention. The number of configurations generated will be the number of values in the user's identifier plus one. This will enable one scrambled, operable keypad to be generated per keystroke required from the user to enter the identifier, plus one for a keypad image. For example, in an embodiment wherein the user's identifier consists of 4 values, the
5 configuration generation component will produce 5 configurations: one for each digit in the identifier and one for generation of the image that the user will see.

Only one operable keypad is 'active' at any given time. Thus, when the user selects (what appears to be) a key on the image, only the active keypad is able to detect the user's input.
10 In an embodiment wherein a plurality of operable keypads has been pre-generated by the device at the start of an authentication session, only one is designated, arranged or executed so as to be the active operable keypad for receipt of the user's next keystroke. After receipt of an input, the active keypad may be altered in some way (eg the keys may be reconfigured) or may be deselected as the active keypad (eg by deletion from memory
15 or removal from the stack).

It should be noted, though, that the user's identifier can be any type or length of identifier, comprising any type of value. It may comprise any type of characters or symbols.

20 At least one image is an image of a default (non-scrambled) keypad. Thus, the 'keys' depicted in the image are presented in a sequential order as expected by the user in conformity with, for example, the standard keypad of the device. In other embodiments, only one underlying, operable keypad may be generated and used to receive all keystrokes from the user. In yet other embodiments, more than one keypad images may be used over
25 the top of one or more operable keypads. This plurality of images may include at least one image of a scrambled keypad. The image may be changed after each input (keystroke) from the user, or may be changed after a predetermined event such as three incorrect attempts. For example, a scrambled image may be used to obtain the user's identifier, but if this is unsuccessful or verification fails, another scrambled keypad image is used and the
30 authentication process is repeated. Upon three unsuccessful attempts using scrambled images, the user may be presented with an image of a non-scrambled keypad.

It should be noted that a scrambled image may be used in conjunction with a scrambled or non-scrambled operable keypad. However, when a non-scrambled image is used, it is arranged to mask a scrambled operable keypad in order to provide the necessary mapping for encoding purposes.

5

Turning to figure 1, the general concept utilised by an embodiment of the invention wherein the keypad configuration is generated on the device, may be expressed as follows.

1. Generate an input string on or at the user's device using biometric data capture or random number generation – see Figure 1, step 101.
- 10 2. Feed the input string into a keypad generation component (KGC) – step 102
3. The generation component uses the input string to generate 5 keypad configurations – step 103
4. Use one of the keypad configurations to generate and display an image of a scrambled keypad, and use the remaining configurations to generate 4 scrambled, operable keypads to underlie the image;
15 superimpose the image 'over' the active operable keypad so that when the user provides an input (keystroke) via the image, the active keypad reads an input into the buffer – step 104
5. Construct encoded version of user's identifier from multiple inputs detected by operable keypad(s) – step 105
20
6. Send encoded version of user's identifier and 5 keypad configurations to remote location for decoding – step 6
7. If the user's inputted identifier is incorrect (ie verification fails), repeat the authentication process; in a subsequent authentication process (eg after three failed
25 attempts) repeat the process using an image of a non-scrambled keypad with a scrambled operable keypad

30

In one implementation, the keypad configurations which are derived from the (random or biometric) input string can be used as inputs to procedure calls which are executed and placed onto the runtime stack.

An illustration of one embodiment of the invention might be expressed as follows:

-23-

```

String input          // input (RN/biometric) used to generate keypad configurations
String usersInput     // (encoded) identifier built from user's keystrokes
int p = 10            // number of keys on keypad
5  int start = 0       // index of start of substring in input
  int end = p - 1      // index of end of substring in input;

input = getInput()    // get input String somehow: random number or biometric data

10 // display image of scrambled keypad using first p chars from input
   generateandDisplayImage(input.substring(start, end))

   // increment start and end indices in the input String
   start = start + p
15 end = end + p

   for (int i = 0; i < N; i++){          // N == length of PIN
       // generate a new keypad using next p values from input
       Keypad k = new Keypad(input.substring(start, end))
20
       //get user's keystroke and add to return String
       usersInput.concat(k.getKeyStroke())

       // increment start and end indices in the input String
25 start = start + p
       end = end + p
   }
   return usersInput // send user's encoded input for decoding and verification

30 In the above illustration, a new keypad is generated as and when required for each
   expected keystroke. In an alternative implementation, a plurality of keypads with different
   configurations may be pre-generated at the start of the session and placed into a data
   structure. The encoded result can then be generated by iterating over that the data
   structure.

35 Stack keypads          // data structure to hold the keypads

   for(int i = 0; i < N; i++){
       //populate the Stack of keypads
40   keypads.push(new Keypad(input.substring(start, end))

       // increment start and end indices in the input String
       start = start + p;
       end = end + p;
45 }

```

-24-

```
for(int i = 0; i < N; i++){           // iterate over the Stack, one key stroke per keypad
    String temp = keypads.pop().getKeyStroke()
    usersInput.concat(temp) // build encoded version of user's input
5  }
```

In yet another implementation, only one mutable, operable keypad object may be generated. The plurality of configurations may then be used to alter the order of the keys in the same operable keypad after each keystroke has been detected.

10

Once the user's encoded identifier has been constructed, it can be sent to a remote server for comparison against the stored version of the identifier. In order to decode the identifier, the server needs to know the mapping of the keys in the keypad(s) and image. Therefore, the keypad configurations generated by the user's device are also sent to the

15

The invention may be implemented on a payment terminal. The payment terminal might incorporate a card-reading component so that data can be read from the chip and/or magnetic strip of an IC card, or via NFC/contactless communication technologies. The

20 payment terminal can be a dedicated device for processing payments and authenticating a user for such transactions. Therefore, such a payment terminal is not a general purpose computing device such as a smart phone or PC. In other embodiments, the invention can be implemented on a non-dedicated device such as a mobile phone, tablet computer, personal computer, lap top etc. This non-dedicated device may be associated with an individual

25

Therefore, the invention provides a secure authentication solution even when implemented on a mobile device. The generation of the keypad configurations on the user's device provides the benefits that processing is performed locally rather than remotely. The

30 combination of biometrics with identifier eg PIN provides a multi-factor authentication which requires the user to be identified on the device ('who the user is') and then authenticated by identifier ('what the user knows'). This alleviates security concerns relating to the use of biometric authentication alone.

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be capable of designing many alternative embodiments without departing from the scope of the invention as defined by the appended claims. In the claims, any reference signs placed in parentheses shall not be
5 construed as limiting the claims. The word "comprising" and "comprises", and the like, does not exclude the presence of elements or steps other than those listed in any claim or the specification as a whole. In the present specification, "comprises" means "includes or consists of" and "comprising" means "including or consisting of". The singular reference of an element does not exclude the plural reference of such elements and vice-versa. The
10 invention may be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device claim enumerating several means, several of these means may be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS:

1. A verification method comprising the step of:
generating an operable, scrambled keypad and providing said keypad within a display
5 zone of a screen associated with an electronic device; presenting an image of a non-
scrambled keypad within at least part of the display zone such that it is superimposed
over the operable keypad, and a user is able to operate at least one key of the keypad
via the image to enable an encoded version of the user's input to be entered into the
electronic device; and
10 constructing an encoded version of a user's identifier from multiple encoded inputs
detected by the operable keypad.
2. A verification method according to claim 1 wherein the operable, scrambled keypad is
generated at run-time by invoking a portion of code.
15
3. A verification method according to claim 1 or 2 wherein the operable, scrambled
keypad is generated by a subroutine which is provided as standard with the device.
4. A verification method according to any preceding claim wherein the image depicts a
20 keypad which is a default keypad associated with the device.
5. A verification method according to any preceding claim wherein:
the image is generated on the device: or
the image is received by the device from a remote computing resource.
25
6. A verification method according to any preceding claim wherein the operable keypad
is generated using a keypad configuration derived using a random, or pseudo-random,
number, or biometric data relating to the user.
- 30 7. A verification method according to any preceding claim wherein the order of the
operable keys in the operable keypad is at least partially determined using biometric
data derived from or associated with the user, preferably wherein the biometric data

comprises, or is processed to provide, one or more strings, arrays or sequences of values which are used to specify the order of the operable keys.

- 5 8. A verification method according to any preceding claim wherein a plurality of operable keypads is generated, and wherein at least one keypad in the plurality is a scrambled keypad.
- 10 9. A verification method according to any preceding claim wherein a plurality of keypad images is generated, and wherein at least one image in the plurality is an image of a non-scrambled scrambled keypad.
- 15 10. A verification method according to any preceding claim wherein a mapping is generated between keys depicted in the image of the non-scrambled keypad and the keys of the operable keypad.
11. A verification method according to claim 10 wherein the mapping enables an encoded version of an input, from the user, to be inputted into the device.
- 20 12. A verification method according to claim 11 and comprising the step of transmitting the encoded version of the input to a remote computing resource.
- 25 13. A verification method according to any preceding claim wherein the electronic device is a mobile phone, a tablet computer, a payment terminal, a portable computing device or a personal computer.
- 30 14. a verification method according to any preceding claim wherein the device is a payment terminal and incorporates a card-reading component so that data can be read from the chip and/or magnetic stripe of an integrated circuit card, or via NFC or contactless communication technologies.
15. A verification system comprising:
an electronic device;

a screen associated with the electronic device;

wherein the electronic device is arranged to:

generate an operable, scrambled keypad and provide said keypad within a display zone of the screen; and

- 5 present an image of a non-scrambled keypad within at least part of the display zone such that it is superimposed over the operable keypad and a user is able to operate at least one operable key of the keypad via the image; and
- construct an encoded version of a user's identifier from multiple encoded inputs detected by the operable keypad

10

16. A verification system according to claim 15 wherein the system is arranged and configured to implement the method of claims 1 to 14.