

Authentication Methods and Systems

This invention relates generally to authentication (verification) of an individual prior to permitting access to a controlled resource or service, and more particularly to biometric
5 authentication. The invention is particularly suited, but not limited to, use in verification of an individual's identity prior to performing a financial transaction.

Authentication methods and techniques are well known. Such techniques include the use of an identifier, such as a PIN or code, which is stored in association with a user. The user
10 is required to supply the correct PIN before being granted access to a controlled resource (eg bank account) or service. The use of PINs has become widely accepted in the banking industry and customers are familiar and comfortable with their use.

Biometric data has also been explored for use with authentication solutions. Biometric
15 data relates to physical or behavioural characteristics of an individual, and can thus be used to uniquely identify that individual. Biometric data may relate to iris, voice, fingerprint recognition and more.

Technologies exist for capturing such biometric data. For example, smart phones have
20 been adapted to include fingerprint scanners. However, the use of biometric authentication has not been widely adopted for use with highly sensitive applications where there is a strong need for security eg the banking industry. One reason for this is that the current banking system and all its infrastructure is geared towards the use of PIN-based authentication. A shift towards biometric authentication would require a very significant
25 investment of time, effort and money to change or replace the existing hardware and software platforms. Another reason is that biometric data may be compromised. For example, there have been cases where fingerprints have been 'lifted' and replicated by third parties. This poses a serious security risk, and while a compromised PIN can be changed, an individual cannot change their fingerprint, voice or iris pattern.

Therefore, it is desirable to provide a solution which combines the convenience of use that biometric authentication offers with the security and logistical advantages of PIN-based authentication.

- 5 Such an improved solution has now been devised.

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

- 10 The invention may provide an authentication method comprising the step:
using biometric data relating to a user (of an electronic device) to provide an encoded or decoded version of an identifier.

Additionally or alternatively, the method comprise the steps:

- 15 capturing biometric data relating to a user;
using the biometric data as input to a software-implemented component which is arranged and configured to use the biometric data to encode an identifier associated with the user such that the biometric data is required to decode the identifier.
- 20 The user's biometric data may be used as, or serve as, a key for encoding the user's identifier. Additionally or alternatively, it may be used or serve as a key for decoding it.

The identifier may be associated with the user, and/or a resource associated with the user.

The resource may be, for example, a payment card such as a debit or credit card, or a

- 25 financial account. The invention is not limited with regard to the type of resource which the identifier is related to. The resource may be a physical resource or an electronic, digital or virtual resource.

The identifier may comprise any type, length or format of identifier. For example, it may

- 30 comprise numerical digits, letters, pictures etc or any combination thereof. Preferably, the identifier is pre-selected (ie determined prior to the authentication process) and stored in

memory on a server. The server may be located at, operated by or on behalf of, a financial institution.

The biometric data may be any type of data relating to the physical and/or behavioural attributes of the user. It may comprise data relating to the user's fingerprint(s), iris pattern, voice, writing, veins or any other biometric source. In this document, the phrase "biometric data" may be used to mean data which is captured directly from the user (i.e. "raw" biometric data such as may be captured by a sensor). Additionally or alternatively, it may 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. This may be a cryptographic key which has been generated during a biometric authentication process, or a registration process involving the capture of the user's biometric data.

Preferably, the biometric data is generated at or on an electronic device operated by the user. The electronic device may be referred to as a 'local' device. Preferably, the electronic device is a handheld, portable or mobile electronic device. It may be a smart phone, laptop or tablet computer, for example. It may comprise wireless communication capabilities for the transmission of data over a local network, close proximity protocol or wide area telecommunications network.

Preferably, the electronic device comprises hardware and/or software capabilities to enable the capture and generation of the biometric data, or is in physical or wireless communication with such a biometric data capture device eg fingerprint scanner, camera, voice recognition software etc. For example, the electronic device may be a smartphone having a camera and voice recognition software, or a finger print scanner built in. Additionally or alternatively, it may comprise an interface to allow the phone to connect to, for example, a scanner.

The biometric data may comprise, or may be processed to provide, one or more strings, arrays or sequences of values. The one or more strings, arrays or sequences of values may be used as, or may be process to provide, a keypad configuration. The keypad

configuration may be a scrambled or randomized keypad configuration. The order of keys in the configuration may be scrambled relative to a default or reference keypad configuration eg the default configuration for the local device.

5 Thus, the biometric data capture device may produce or comprise a series of values, or the output of the biometric device may be processed to provide the series of values. Those values may be used as the labels assigned to keys in a keypad or keypad image. Thus, the biometric data may be used as, or to specify, a keypad configuration. Hereafter, the series of values may simply be referred to as an array. The array may be a portion or substring of
10 the biometric data. The invention is not to be limited in respect of the data type, length or format of the biometric data or the array(s) generated from the biometric data.

The biometric data may be provided to a keypad generation component (KGC). The KGC may be a component provided on the local device or in communication with the local
15 device. It may be a software application. The keypad generation component may be arranged to generate a Pin Entry Device (PED).

The biometric data may be used as input into a software component provided either on a handheld device operated by the user or on a remote computing resource such as a server.
20 The software component may be arranged to use the biometric data to encode the identifier, or to use it as a seed for an algorithm arranged to generate a keypad configuration and/or a PED. The software component may be arranged to perform an encryption and/or randomisation process.

25 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 to generate the seed. The key may be a private or public cryptographic key which is associated with a user and/or a digital wallet associated with a user. The
30 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.

Preferably, the encoding and/or decoding process may be performed using an altered or randomised keypad configuration, although any suitable encoding/decoding method could be used which is dependent upon the biometric data.

5

In one or more embodiments, the method may further comprise the step of using the biometric data to generate at least one operable keypad and/or at least one keypad image.

The layout of the at least one operable keypad and/or at least one keypad image may be determined using the biometric data or a portion thereof. Therefore, the biometric data

10 may serve as or be used to supply the keypad configuration for the operable keypad and/or image. The keypad/image generation step may be performed by the KGC which may be arranged and configured to receive the biometric data and process it to provide the one or more operable keypads, and/or one or more keypad images.

15 Preferably, the arrangement or configuration of keys in the operable keypad is different relative to the arrangement or configuration of keys depicted in the keypad image. The operable keypad is a functional keypad comprising a plurality of keys, each key having a value or symbol associated with it upon creation of the keypad, such that when a key is selected its associated value is placed into memory. The keypad may be an object
20 generated electronically. It may provide a model or representation of a mechanical keypad. The keypad object may be generated using a subroutine (procedure, function or method) call. The subroutine may use parameters to determine the arrangement (order, position) of keys in the keypad. Upon execution of the procedure or method, the keypad object may reside in volatile memory until it is discarded. The operable keypad may be or
25 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.

By contrast, the keypad image may be a representation of a keypad and devoid of
30 functionality in itself. Therefore, in the absence of an operable keypad, the user is not able to input any values into memory by selecting the ‘keys’ depicted in the image. 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.

As the arrangement of keys in the operable keypad is preferably different relative to the
5 arrangement of keys depicted in the keypad image, the type, order and/or position of the
operable keys does not correspond exactly to the type, order and/or position of the 'keys'
depicted in the image. The keys in either the operable keypad or the keypad image may be
scrambled relative to a reference keypad. As the order of keys in the operable keypad is
preferably different to the order of keys depicted in the image, a mapping may be
10 generated between the operable keypad and the image. This mapping may be used to
encode and/or decode the identifier.

Preferably, the at least one operable keypad and/or at least one keypad image are provided
within a display zone of the electronic device used to capture or generate the biometric
15 data. The display zone may comprise a portion of a touchscreen. Advantageously, they
are provided within the same display zone such that the keypad image superimposes or
masks the operable keypad which underlies the image. Thus, the keypad(s) and/or
image(s) may be generated by procedure calls; the image may be presented such that it
blocks or obscures the keypad from the user's view at least partially but preferably
20 completely. Therefore, the user may see what they believe to be a keypad and may select
eg by touching what they believe to be an operable key with a given value, while in reality
they are simply touching a portion of an image. By 'selecting' a portion of the image,
however, the user may cause an operable key of the keypad to function, and thus the value
that is placed into memory by the operable keypad may not correspond to the value that the
25 user intended to input. Therefore, an encoded version of the user's identifier may be
generated due to the mapping between the keys in the keypad and those depicted in the
image. An advantage of this is that the user's 'real' identifier is never placed into memory
on the local device. Therefore, it cannot be accessed by an unauthorised third party who
has managed to compromise the local device.

30

This encoding aspect of the invention may be substantially as described in WO
2014/013252 which discloses an authentication solution wherein an image of a scrambled

keypad is superimposed over an operable keypad to provide an encoded version of an identifier. However, in accordance with the present invention the keypad(s) and or image(s) may be generated at or on the local device using biometric data.

5 Thus, the at least one operable keypad and/or the at least one keypad image generated using the user's biometric data may be used to provide an encoded version of the user's identifier. The encoded version of the identifier may be transmitted from the local device to a remote device (eg server) where it may be stored. It may be stored in secure storage. It may be transmitted wirelessly.

10

The keypad image may be generated such that one or more of the keys depicted in the image are colour coded, tagged or otherwise marked (in addition to the value associated with the key). As the biometric data ensures that the same array package and therefore the same image may be generated each time, the marked keys may provide a visual

15 reassurance to the user that the image they are viewing is legitimate rather than the result of unauthorised activity on the local device. For example, the user may expect that the key in the top left corner of the image is coloured yellow and the middle key on the bottom row of the keypad image is coloured red. If this is not the case then the user may suspect that the image has been provided by an unauthorised party.

20

The identifier may be encoded as part of a registration process wherein a user registers to use an embodiment of the invention. The encoding may be performed only once in respect of the same identifier. The registration process may comprise the capture of non-biometric data relating to the user, and/or data relating to a resource associated with the user eg a

25 credit card number. In the event that the user changes the pre-stored version of the identifier (eg via their financial institution), an encoded version of the user's new identifier may be provided using the process described above and may be stored in place of the previously encoded version.

30 The biometric data may be used to determine the configuration of keys in the operable keypad and/or the configuration of keys depicted in the keypad image. This may be achieved by using the biometric data as input into the procedure, function or method call(s)

used to generate the at least one operable keypad and/or the at least one keypad image. The procedure or method call(s) may form part of the keypad generation component. The keypad configuration component may generate the keypad(s) and image(s) on or at the local device. The biometric data may be used to provide one or more arrays of values,
5 each array corresponding to a keypad configuration for creation of a keypad or image. The biometric data may be processed to provide the one or more arrays.

A plurality of operable keypads may be generated by the keypad generation component. Additionally or alternatively, a plurality of keypad images may be generated. The
10 configuration of keys in each keypad or image may be different from the others in the respective plurality. One keypad and/or image may be designated as the 'active' keypad or image at any given time. For example, one keypad image may be used during an authentication session while a different underlying keypad may be used per keystroke received from the user. In some embodiments, one mutable keypad may be used and the
15 state of the keypad may be altered so as to provide a different configuration of keys. Additionally or alternatively, the underlying operable keypad may remain the same during the authentication process while the keypad image may change.

At a minimum, one operable keypad or one keypad image is generated on the local device
20 using the biometric data to determine its configuration. Additional configuration data and/or images may be sent to the local device from a server. For example, the biometric data may be used to generate an operable keypad at the local device and the keypad then superimposed with a keypad image received from a server. Alternatively, the keypad configuration data may be received at the local device from a server while the image is
25 generated on the local device using the locally captured biometric data. However, in a preferred embodiment, the image(s) and keypad(s) may all be generated at the local device. This is advantageous because it eliminates the risk of the configuration data being intercepted during transmission to the local device, and because it transfers the processing burden from the server to the local device.

30

As an individual's biometric data does not change, the same encoded version of the identifier and/or keypad configuration will be generated each time a given user uses the

- invention. Another advantage is that as the user's biometric data can be used to determine the mapping between the keys in the operable keypad and the keys depicted in the keypad image, the user's biometric data becomes the 'key' for decoding the encoded version of the user's identifier. A further advantage is that as the user's biometric data can always be
- 5 captured or re-generated, it does not need to be stored. Thus, once the encoded version of the identifier has been created and stored, it can always be decoded upon supply of the user's biometric data. This avoids the need for the user to carry any additional authentication devices, such as hardware tokens, or remember any further information in order to decode the identifier. The user always carries the key to unlock the identifier.
- 10 The invention therefore provides a multi-factor authentication solution which requires biometric data (who the user is) and an identifier (something the user knows). When the identifier relates to a resource eg the user's payment card (something the user has) this provides a three-factor authentication solution.
- 15 The method may also comprise the step of using biometric data relating to the user to compute a decoded version of the encoded identifier. This decoding step may be performed following the registration process described above during which the encoded version of the user's identifier may be generated and stored. The decoding step may be performed as part of an authentication session initiated when the user wishes to gain access to a controlled
- 20 resource or service, or perform a transaction. The decoding step may also be performed during the registration process to verify that the user's inputted identifier is correct ie matches a pre-stored version of the identifier.
- The biometric data used to decode the encoded identifier may be captured separately from
- 25 and subsequently to the biometric data used to produce the encoded version. Computing the decoded version may involve the use of one or more strings, arrays or sequences of values generated from biometric data relating to the user. The decoding may be performed by or at a server. The decoding may be performed within a HSM associated with a server.
- 30 The decoded version of the identifier may be verified in relation to a previously stored version of the identifier. The previously stored version may be stored by an institution or party associated with a payment card. The verification may be performed by sending a

payment message or balance enquiry to a financial institution. Verification of the identifier may be successful if the decoded version of the identifier matches the previously stored version, and unsuccessful if it does not match.

5 Advantageously, only the user's biometric data is required in order to decode the identifier. Re-input of the user's identifier is not required. Neither is generation of the image or operable keypad required again. Preferably, after the encoded version has been stored (and optionally verified) on a remote device, eg server, the user may only need to re-input their biometric data eg swipe finger so that the arrays may be re-generated and transmitted to the
10 server for decoding of the identifier. The arrays may enable the server to know the mapping between the configurations of the reference keypad and the keypad and/or image generated using the biometric data. Also advantageously, the biometric data and the arrays generated from it do not need to be stored. This provides a more secure solution as the key to decode the identifier cannot therefore be accessed from storage.

15 Also in accordance with the invention, there is provided an authentication system arranged and configured to implement any embodiment of the method described above. Such a system may comprise an electronic device arranged and configured to encode an identifier using biometric data relating to a user of the device.

20 The biometric data may be generated at or on the electronic device. The electronic device may be a handheld, portable or mobile computing device. The device may be arranged and configured to generate one or more strings, arrays or sequences of values from the biometric data.

25 The device may be arranged to implement the encoding process described above or any other encoding process that uses the biometric data to serve as a key. It may be arranged to use the biometric data to generate or specify a keypad configuration. The keypad configuration may be used to generate at least one operable keypad and/or at least one
30 keypad image. The configuration of keys in the operable keypad may be different relative to the configuration of keys depicted in the keypad image; and/or

the at least one operable keypad and/or at least one keypad image may be provided within a display zone of the electronic device used to capture or generate the biometric data.

5 The biometric data may be used to determine the configuration of keys in the at least one operable keypad and/or the configuration of keys depicted in the at least one keypad image. The at least one operable keypad and/or the at least one keypad image may be used to provide an encoded version of the identifier. The system may comprise memory for storage of the encoded version of the identifier; preferably wherein the memory is provided on or at a server.

10

The at least one keypad and/or at least one keypad image may be generated using at least a portion of the biometric data as input into a method or procedure call. The at least one operable keypad may be at least partially masked or obscured from the user's view by the at least one keypad image.

15

The system may comprise a further device arranged to compute a decoded version of the encoded identifier using biometric data relating to the user. Computing the decoded version may involve the use of one or more strings, arrays or sequences of values generated from biometric data relating to the user. The system may be arranged to verify
20 the decoded version of the user's identifier in relation to a previously stored version of the identifier.

The invention may provide an authentication method comprising the steps of:
generating an operable keypad or keypad image more than once, wherein the configuration
25 of keys in the keypad or image are altered relative to a reference configuration of keys; and
colour coding or otherwise altering one or more pre-selected keys in the keypad or image such that the same key or key position is always altered in the same way each time the keypad or image is generated. This aspect, as described above, may provide an assurance to a user that the keypad and/or image has been generated by a legitimate
30 source.

It should be noted that any feature described above in relation to one aspect or embodiment of the invention may also be used to advantage in relation to any or all other aspects or embodiments. For example, a feature described in relation to a method of the invention may also be applicable to a system or apparatus in accordance with the invention, or vice versa.

These and other aspects of the present invention will be apparent from and elucidated with reference to, the embodiment described herein.

10 An embodiment of the present invention will now be described, by way of example only, and with reference to the accompany drawings, in which:

Figure 1 is a flowchart showing the process of using biometric data to generate an image and a plurality of keypads to capture a user's keystroke, in accordance with the invention.

15 Figure 2 shows part of the registration process in accordance with an embodiment of the invention.

Figure 3 shows part of a post-registration process in accordance with an embodiment of the invention.

Figure 4 shows an overview of at least some of the steps which may be used in accordance with an embodiment of the invention.

25 An illustrative embodiment of the invention will now be provided in relation to the banking industry. It also uses an encoding process which involves the use of a randomised keypad and/or keypad image generated at least in part using the biometric data. However, it should be noted that the invention is not limited in these respects.

30 A method according to one embodiment of the invention comprises a two-step process. The first step comprises a registration process which is used to generate and store an encoded version of a user's identifier. The identifier could be any type of code or

password associated with the user. The user's biometric data is used to generate the encoded version. Following registration, the user's biometric data is used to decode the encoded version of the identifier each time the user wishes to authenticate with a service or system. Therefore, the user's biometric becomes the key to unlock the encoded version of the identifier. The user's biometric data does not need to be stored but can be captured upon demand when required. This provides a more secure but convenient authentication arrangement, which does not require alteration of existing infrastructure.

Figure 4 shows an overview of at least part of the process of the present invention. As shown, a user's biometric data (eg fingerprint) is captured by a capture device 19. This is stored in a secure storage element on the user's device 20. The biometric data and/or the user's private key are used to generate a seed 21. The seed is used as input into an algorithm which generates a number of arrays which can be used to generate a PED 22. Thus, the PED generation is dependent upon the user's unique biometric data.

Registration process

The user is required to register with the system before first use. Part of the registration process is shown in Figure 1. During registration the user may need to supply data such as name, address and data relating to one or more payment cards. This data may be stored on a remote device such as a server, or on the user's (local) device. The local device may be any type of computing device such as a mobile phone, laptop computer, PC, tablet computer. The registration data may be stored in a digital wallet provided on the local device. As is known in the art, the wallet may comprise or be associated with a cryptographic private/public key pair. The key pair may have been generated during set up or registration of the wallet using a biometric capture process.

The local device either includes or is in communication with a biometric capture device. Various types of capture device are known in the prior art and the invention is not limited with regard to the type of data that is captured or the type of device used to capture it. The following example refers to fingerprint data and fingerprint scanners but other types of biometric data and their respective capture devices may be used instead or additionally.

The fingerprint scanner is used to capture the user's biometric data 1. This is then fed into a Keypad Generation Component (KGC) provided on the local device. The KGC may be a software application which is downloaded to the local device for installation from a remote source such as a cloud-based server. The biometric data is provided to the KGC as an
5 input string. The string can be used to provide one or more arrays of values 2, each array (or part/element thereof) capable of serving as input to a procedure call. The arrays may be substrings of the String produced from the biometric capture step 1. In a preferred embodiment, the KGC processes the biometric input string to generate a package of $N+1$ arrays wherein N is the number of digits in the user's identifier 3. The additional array can
10 be used to generate a keypad image. Each array specifies the order (ie configuration) of keys in the image or keypad. These arrays may be stored in secure temporary storage.

In step 3, the KGC takes the input string and uses it to make a plurality of procedure calls. The first procedure call is to an image generation procedure which takes one array (ie part
15 of the input string) and generates an image of a keypad. Thus, the biometric data is used as the parameters to the procedure call. The parameters dictate the configuration of keys depicted in the image. The term 'configuration' may relate to the position, order and/or arrangement of the 'keys'. The image is then displayed within a display zone of a screen associated with the local device. In this example, the local device is a smart phone having
20 a touchscreen although a PC, monitor and mouse may be used to equal effect.

The image is created such that it resembles the style of a (default) keypad associated with the local device. However, in one embodiment the keys depicted in the image are scrambled relative to the device's default keypad. In other embodiments, the image may
25 depict a non-scrambled keypad.

In one or more embodiments, the keypad image is arranged such that one or more keys are colour coded or otherwise tagged, marked or identified (besides the value associated with the key). This enables an image that is visually unique to the user to be generated. For
30 example, certain keys can be given a background colour. This can be used as a visual reassurance to the user that the image they are seeing is from a legitimate source rather than something presented by an unauthorised party that has compromised the local device.

The KGC also makes one or more calls to a keypad generation procedure using one or more other portions of the biometric data as input. In a preferred embodiment, a plurality of operable keypads is generated, one keypad for each value or digit in the user's identifier.

5

An operable keypad is generated by the procedure and provided within the same portion of the screen as the image. Preferably, the image covers the keypad completely so that the user is unable to see the operable keypad due to the image that superimposes it 4. The configuration of keys in the operable keypad is different from the configuration of keys depicted in the image. At least one key is in a different position, although preferably more than one or all positions are different. Therefore, there is a mapping between the keys in the operable keypad and those depicted in the image. This mapping is dictated or at least influenced by the biometric input and therefore the encoding and subsequent decoding is dependent upon the biometric input.

15

In one embodiment, the image may depict a non-scrambled keypad while the keys in the underlying operable keypad are scrambled. In another embodiment, the image may depict a scrambled keypad while the keys of the underlying operable keypad are not scrambled. In yet another embodiment, both the keys depicted in the image and the keys of the operable keypad are positionally scrambled.

20

The user enters the first digit of their identifier which is associated with the payment card that they are registering, by 'selecting' the first digit on the screen 5. However, as the image comprises no keypad functionality in and of itself, and as the image is masking the operable keypad which is monitoring the screen for input, the user causes a key of the hidden keypad to operate. The value associated with the operated key is placed into memory on the local device 5. Thus, the value that is actually stored by the keypad may not correspond to the value that the user "selected" in the image. An encoded version of the input has been generated and can only be decoded if the mapping between the keypad and image configurations is known.

30

This input process (step 5) is repeated for each digit in the user's identifier so that a complete encoded identifier can be constructed in memory by concatenating each input to the previous inputs 6. In one embodiment, only one mutable keypad is generated but the configuration of keys is altered during the process. Arrays derived from the biometric
5 input are used to alter the state of the keypad. In another embodiment, the underlying keypad is replaced for each keystroke so a new keypad with a different configuration is used for each input. Thus, the keypad generation procedure may be called more than once, each call using a (different) array of values derived from the biometric data. In some embodiments, the image may be replaced during the input process. In some embodiments
10 the biometric data may be used to specify the scrambled configuration of only the operable keypad, or only the image. In other embodiments it may be used to scramble the configurations of both the displayed image and the hidden keypad.

As the same user will always provide the same biometric data, the same string and
15 therefore image and/or keypad configuration(s) will always be generated.

Turning to figure 2, when an encoded version of the user's complete identifier has been constructed 6, it is stored in secure storage on the user's device along with the N+1 arrays that were used to create it. A copy of the encoded identifier and arrays is sent to a server 7
20 and passed to a Hardware Security Module (HSM) 8. The HSM is located remotely from the local device, at a server. Where the identifier is associated with a card such as a credit or debit card, it is necessary to check that the identifier entered by the user is the correct one for the card. Therefore, it must be verified with the card's issuing institution.

25 To perform the verification, the encoded identifier is decoded using the array package that was used to create it 8. This decoding is possible because the array package provides the mapping between the image and keypad configurations. The un-encoded version of the identifier is then stored in the HSM, and is used to generate a PIN block. The PIN block is used to send a payment message to an acquiring institution which then relays it to the
30 card's issuing institution 9.

If the identifier is not correct 12 (ie does not match the identifier stored in association with that card by the issuing institution) the issuing institution will respond with a message indicating this. The user can then be asked to re-enter his identifier and the process described above is repeated. If three incorrect identifiers are inputted, the registration
5 process may be aborted 13.

If, however, the issuing institution indicates that the identifier is correct 10, the encoded version of the identifier is moved from temporary storage to secure storage 11. The temporary storage is then erased.
10

It should be noted that the identifier can be verified in a variety of ways. In one embodiment, a balance enquiry can be generated at the server and sent to issuing institution over the ATM network.

15 When the registration is complete, an encoded version of the user's identifier for a given card has been generated and securely stored. As the encoding was performed using a mapping generated from the user's biometric data, the biometric data is the key required to unlock or decode the identifier. The array package does not need to be stored anywhere, either at the local device or on the server, as it can be generated upon demand by re-
20 capturing the user's biometric data. Similarly, the user does not need to re-enter the identifier during subsequent authentication sessions because the encoded version has been securely stored on the server. Therefore, only the array package needs to be generated during subsequent authentications and sent to the server so that the previously stored, encoded identifier can be decoded. This provides a secure and convenient authentication
25 solution.

Authentication after registration

As shown in Figure 3, after registration, when the user wishes to perform a transaction using the registered payment card, the card is selected from the digital wallet on the local
30 device. He scans his fingerprint 14. The string generated from the biometric capture is fed as input into the KGC as above. The N+1 arrays are generated and sent to the server 15 where they are placed into temporary storage. The previously verified, encoded identifier

is retrieved from secure storage 16. The encoded identifier and arrays are put into the HSM 16 where the arrays are used to decode the identifier 17. The identifier and card details (which are retrieved from the wallet or entered when required by the user) are sent with the transaction amount to an acquiring institution e.g. bank as a payment message 18.

- 5 The acquiring institution then relays the message to the issuing bank which will process the transaction if the identifier is correct or decline it if the identifier is incorrect.

Thus, the decoding process does not require any input from the user other than the biometric data. The identifier does not need to be re-entered, and the keypad(s)/image(s)
10 do not need to be re-generated.

In one or more embodiments, the encoding process may be performed by a different party from the decoding process. The identifier may be encoded using the biometric data and then supplied to another party and stored, in encoded form, on a further system or device.

- 15 The other party then only requires the user's biometric data, which can be captured and supplied as required, to unlock the identifier.

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
20 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 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
25 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 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.
30 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. An authentication method of encoding and/or decoding an identifier using a scrambled configuration of keys in an operable keypad and/or image of a keypad, comprising the steps:
 - 5 using biometric data relating to a user to provide an encoded or decoded version of an identifier by using the biometric data to provide one or more strings, arrays or series of values, each corresponding to a keypad configuration for the creation of a keypad or image of a keypad; and
 - 10 using the one or more strings, arrays or series of values as input to a subroutine call, wherein the subroutine comprises instructions to generate the operable keypad and/or the keypad image; and the biometric data determines or is used to supply a scrambled configuration of keys in the operable keypad and/or a scrambled configuration of keys depicted in the keypad image.
 - 15
2. A method according to claim 1 and further comprising the step:
 - generating the biometric data at or on an electronic device.
3. A method according to claim 2 wherein the electronic device is a handheld, portable or mobile computing device.
 - 20
4. A method according to claims 1, 2 or 3 and comprising the step of:
 - using the biometric data to encode the identifier such that the biometric data becomes the key to decode the identifier.
 - 25
5. A method according to any preceding claim, wherein:
 - the subroutine forms part of a keypad generation component arranged to generate the at least one keypad and/or keypad image on or at an electronic device operated by the user.
 - 30

6. A method according to any preceding claim and further comprising the step:
storing an encoded version of the identifier.
7. A method according to claim 6, wherein the encoded version is generated using a
5 keypad configuration specified by the biometric data; and/or
the encoded version of the identifier is stored on a server.
8. A method according to any preceding claim and comprising the step:
generating at least one operable keypad and at least one keypad image, wherein:
10 the configuration of keys in the operable keypad is different relative to the
configuration of keys depicted in the keypad image.
9. A method according to any preceding claim and comprising the step of:
using the biometric data to compute a decoded version of the encoded identifier,
15 wherein the decoding step is performed as part of an authentication session initiated
when the user wishes to gain access to a controlled resource or service, or perform a
transaction.
10. A method according to any preceding claim and further comprising the step:
20 verifying the identifier by comparing it to a previously stored version.
11. A method according to any preceding claim and further comprising the step of:
sending the biometric data, or data derived from the biometric data, from an electronic
device operated by the user to a remote computing resource.
25
12. A method according to claim 11 wherein:
the biometric data is sent to the remote computing resource to enable an encoded
version of the identifier to be decoded using the biometric data or data derived
therefrom.
30
13. A method according to any preceding claim, wherein:
the order of keys in the scrambled configuration of keys in the operable keypad and/or

the scrambled configuration of keys depicted in the keypad image is scrambled relative to a default or reference keypad configuration.

14. An authentication system comprising:
- 5 an electronic device operated by a user; and
 a remote computing resource;
- wherein the system is arranged and configured to use biometric data relating to a user
 to provide an encoded or decoded version of an identifier by:
- using the biometric data to provide one or more strings, arrays or series of values,
10 each corresponding to a keypad configuration for the creation of a keypad or image
 of a keypad; and
- using the one or more strings, arrays or series of values as input to a subroutine call,
 wherein the subroutine comprises instructions to generate the operable keypad and/or
 the keypad image; such that the biometric data determines or is used to supply a
15 scrambled configuration of keys in the operable keypad and/or a scrambled
 configuration of keys depicted in the keypad image.
- 15 . A system according to claim 14 wherein:
- the biometric data is generated or captured at or on the electronic device.
- 20
- 16 . A system according to claim 15 wherein the electronic device is a handheld, portable
 or mobile computing device.
- 17 . A system according to claim 14, 15 or 16 , wherein the system is arranged to:
- 25 encode the identifier using the biometric data such that the biometric data becomes the
 key to decode the identifier.
18. A system according to any of claims 14 to 17 wherein the system is arranged and
 configured to perform the method of any of claims 1 to 13 .
- 30