

-1-

Authentication Method and System

This invention relates generally to the field of user authentication, and more particularly to the field of PIN-based verification. The invention is suited for use in situations where a user is required to enter a code, such as a Personal Identification Number (PIN), which is validated prior to completing an operation. The operation might be any type of operation.

Authentication is a technique 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 (such as a code or combination of symbols) which is then maintained in secrecy in a secure location and available only to authorised parties. The identifier is stored in association with a particular user or group of users, and may sometimes be stored and/or used in conjunction with another pre-determined identifier such as a username, for example. The identifier is often selected by the user himself although sometimes it may be the resource manager or owner who determines it. The user may, in many cases, be able to change their previously selected identifier. Often, the identifier is chosen when the user initially joins an organisation; for example, when he begins employment at a certain company, or registers with a provider for a certain service. After the identifier has been selected and assigned to an authorised individual, that user is required to supply the pre-determined identifier each time he requests permission to perform the controlled act or gain access to the resource or service. The user's inputted identifier is compared with the stored version. If the user is able to supply the correct identifier then his identity is deemed to have been verified and access is granted. If, on the other hand, the correct identifier is not supplied then access is denied.

In this document such an identifier may be referred to as a Personal Identification Code (PIC).

-2-

One common example of a PIC is a 4 digit numeric code typically referred to as a Personal Identification Number (PIN). The term 'PIC' is intended to include the term 'PIN' (Personal Identification Number). However, other codes of different lengths and containing different types of characters or symbols may be used. The present invention is
5 not intended to be limited with regard to the length of the identifier used, or the type of characters it contains. For example, it may contain numeric digits, alphabetical characters, pictures, punctuation or any other kind of symbol, or a mixture thereof. The term 'PIN' or 'PIC' may be used hereinafter to refer to the user's identifier for the sake of convenience but should not be construed as being limiting in any way as to the length, type or format of
10 the identifier.

PIN-based verification systems typically comprise a keypad which enables the user to enter their pre-selected PIN. A typical keypad layout known in the art is shown in Figure 14a. A keypad is a set of buttons or 'keys' arranged in a block or 'pad'. The keys are set out in
15 a grid adjacent one another to form the pad. The keys have indicia (identifiers) printed, engraved, embossed or otherwise displayed on them. The indicia on a key typically consists of one symbol e.g. '6' but could comprise more than one symbol e.g. 'AB'. The indicia on the keys are usually arranged in an ordered manner, such as a sequential series. For example, numeric digits would typically be ordered in ascending order. In this
20 document, the term 'keypad' may be used interchangeably with the term 'pinpad'.

Keypads are often found on alphanumeric keyboards connected to computing devices. Other devices such as calculators, push-button telephones, combination locks, and digital door locks are also known to comprise a keypad. The advent of portable
25 telecommunications and computing devices has also seen keypads introduced into mobile devices such as mobile (cellular) telephones, tablet computers, PDAs and so on.

Many electronic devices now include computer processing capabilities and a touch screen interface capable of displaying a keypad. These may be used for a variety of purposes,
30 including allowing an authorised user to 'unlock' the device by entering a passcode comprising a combination of pre-selected symbols, or entering a telephone number so as to

-3-

make a call. Card-reading terminals used in financial transactions also have keypads to allow the user to enter his PIN via the keypad.

Each type of smart phone (e.g. brand and/or model) may have a particular style of keypad associated with it as its 'default' keypad. For example, the keys may be arranged in a particular format or layout, or a particular font may be used for the indicia. Therefore, the user of an electronic device may become familiar with a certain 'look and feel' with respect to the keypad on that device. An example of a typical keypad generated and displayed on a widely known smart phone is shown in Figure 14b. The default keypad is generated by the execution of a procedure call within the phone.

In contrast to conventional keypads which have depressible (physically movable) keys, a touch screen can be used to display an image of a keypad having numbered or otherwise indicated 'hot spots' corresponding to the physical keys of the conventional counterpart. The user touches the hotspots corresponding to the keys of his choice instead of pressing a moveable key. Sensors placed below the surface of the screen sense which area(s) have been selected by the user, thus 'reading' the user's input.

Perhaps the most common use of keypads and PIN-based technology is in relation to financial transactions e.g. automated teller machines (known as 'ATMs' or 'cashpoint machines') and point of sale devices for banking cards (i.e. debit cards and credit cards).

Prior to the introduction of PIN-based authentication, if a customer wished to make a purchase for goods or services, he would be required to provide a signature which would be compared to the signature on the back of the card. However, signatures can be forged with relative ease.

In order to address this problem, smartcard technology has been introduced in many countries for credit, debit and ATM cards. This payment system (sometimes known as the 'chip and pin' system) is based on a global standard known as the EMV standard. Using this approach, credit and debit cards are provided with an embedded microchip. When a customer wishes to pay for goods using this system, the card is placed into a "Point of

-4-

Sale" terminal or a modified swipe-card reader, which accesses the chip on the card. Once the card has been verified as authentic, the customer enters a 4-digit PIN, which is submitted to the chip on the smartcard; if the two match, the chip tells the terminal the PIN was correct, otherwise it informs it the PIN was incorrect. The inputted PIN matches the
5 stored PIN if each symbol in the input is also found in the stored version, and in the same order and number.

In certain situations financial transactions may be carried out by swiping the magnetic stripe on the card so as to read the card's data, or by manual entry of the card details, rather
10 than by inserting the card into a dedicated card-reading device.

It should be noted that as the PIN is sent back to the host for verification, security considerations become relevant because the PIN can be intercepted during the transmission process.
15

Since the introduction of PIN-based verification, fraud arising from face-to-face transactions (where the card and the customer are physically present at the retail site where the transaction takes place) has been drastically reduced because it is significantly more difficult to fraudulently obtain or guess a PIN than it is to forge a signature.
20

Moreover, prior to the advent of PIN-based authentication, if a customer's signature was forged, the card provider was usually held legally liable for any ensuing fraud and was compelled to reimburse the customer. With the introduction of smartcard technology, however, the onus has typically shifted to the customer to prove that they had acted "with
25 reasonable care" to protect their PIN, rather than on the card provider being required having to prove that the signature provided during the transaction matched that on the card. This transfer of liability provides very significant financial benefits for card providers.

Another drawback of signature-based verification is that it does not lend itself to
30 transactions where the card (and the customer) is not present at the retail premises when the transaction is performed – for example, transactions made over the telephone or internet. Such transactions are usually known as 'card not present' (CNP) transactions.

-5-

CNP transactions are now commonplace in today's retail environment, with many customers choosing to conduct financial operations without being at the retail location. However, while PIN-based technology provides a relatively secure authentication solution for 'card present' face-to-face transactions, fraud arising from CNP transactions is rising.

5

In addition, mobile (cellular) telephone technology has opened new opportunities for retailers and consumers alike. So-called 'smart' phones comprising sophisticated computing capabilities and have become extremely popular, offering the user facilities such as the ability to surf the web and view retailers' web sites. Customers and retailers alike are often not tied to one physical geographical location but are 'on the move'. For example, customers may wish to make a purchase via a web site being viewed on a mobile phone while waiting at a bus stop; or a parking attendant may wish to take payment from a driver in a car park. In such cases, dedicated Point-of-Sales terminals are not available for use.

15

However, despite the enormous popularity of mobile computing technology, in particular telephones, its use in respect of CNP transactions has been limited due to security concerns as data (such as the user's PIN) can be intercepted during transmission from the device to/from the card provider's server, or whilst residing in the phone's internal memory.

20

Some PIN related technology has been designed with mobility in mind and is known in the prior art.

For example, CardEase Mobile® is a mobile payment app which, in conjunction with a mobile card reader, enables a retailer to take Chip and PIN mobile card payments from a customer. The retailer enters the amount of the purchase into an app downloaded and installed on his mobile phone (or tablet device). The retailer then gives the card reader device to the customer who swipes or inserts his credit/debit card into the reader, and enters his PIN via the keypad on the reader device. The reader then connects via Bluetooth to the app on the retailer's mobile device, which then connects to the service provider via the phone's internet connection for payment authorisation. Once the payment has been

30

-6-

approved, the customer removes his card from the reader and the retailer emails or texts a receipt to the customer.

However, this known arrangement requires the use of the card reader. In effect, it uses the
5 mobile phone to play the role of the point-of-sale terminal which would usually be located within the store/shop. The merchant taking the payment still needs to be at the same location as the customer making the payment because he must hand the card reader to the customer for use with his credit or debit card. The system does not eliminate the need for a dedicated (i.e. purpose built) card-reading device.

10 Another example of the prior art is disclosed in WO/2012/004395 A1 ('iZettle'). The iZettle arrangement comprises a portable card reader device for reading a smart card, a portable reader device and a payment server. The aim of the disclosed method is to eliminate the unsecure keyboard in a mobile phone used for entering a PIN, and instead use
15 a separate PIN entry device which fulfills the EMV level specification. In essence, the disclosed approach uses an external PIN pad provided with all the required secure chips and components and which simply communicates with the mobile phone via a Bluetooth connection. Thus, as above, the iZettle disclosure does not solve the problem of using unsecure mobile devices for PIN entry, it simply circumvents it by using a separate PIN
20 entry device.

Indeed, the iZettle document states (lines 6 to 19) that:

'A more practical solution would be if a credit card payment could be conducted using a well-known, non-bulky and commonly used device such as a
25 mobile phone. However, an ordinary mobile phone does not have a built-in card reader where you could swipe your credit card, and even if that particular problem could be overcome, there is still an issue regarding the level of security a mobile phone provides. It is well known that for instance a spy program could infiltrate the mobile phone and hijack credit card information
30 and identification information, such as the PIN code entered into the mobile phone via the phone's keyboard when conducting a credit card payment, without the user even knowing it. In light of the above, a standard mobile

-7-

phone is generally not considered to be a secure device, and thus not suitable for making credit card payments with. Thus, finding a way to make secure credit card payments with a mobile phone is highly sought after’.

- 5 Another known arrangement (also from the applicant of WO/2012/004395 A1) comprises a device (‘dongle’) and associated software which fits into the charging port of a smart phone. When a transaction is to be made, the customer’s card is inserted into the dongle. The customer is then asked to sign the phone’s touch screen with their finger in order to authorise the transaction. Using this approach, the user does not need to enter a PIN.
- 10 Therefore, the problem of PIN entry on an insecure portable device is avoided rather than solved.

- Yet another known approach is disclosed in WO 2011/093998 A1. Again, the disclosed approach uses a dongle-based card reader which is plugged into the device. It does not
- 15 provide a secure technique for enabling PIN-based authorisation.

- GB 2416058 A discloses an approach for verifying a request for access to a server. In response to an access request, a random string of characters is generated by a ‘combination generator’ in a security server. It then uses this random string to generate ‘image data’
- 20 which is sent from the server to the user’s computer. The keypad on the user’s computer is then modified in accordance with the image data. The user then enters his PIN using the modified keypad displayed on the computer. Positional data relating to the user’s selection within the grid of keys (e.g. first-row-first-column) is stored as a record of the user’s PIN. The positional data is then converted by the user’s machine into character data such as a
- 25 string of digits to form an encoded PIN which is then sent to the server for verification. However, the encoded PIN can be ‘decoded by knowing the image data’ – lines 22, 23 of page 10. Therefore, as the image data is stored on the user’s computer, if the security of the user’s machine is compromised (e.g. hacked into, or is infected with malware) access may be gained to the image data, therefore enabling a third party to decode the user’s PIN.

-8-

Thus, it is desirable to provide an authentication method which does not render the PIN vulnerable to unauthorised access during transmission between devices, or when stored temporarily in an electronic device during the verification process.

5 Ideally, a PIN-based authentication solution which would enable a user to complete a CNP transaction using a PIN to authenticate in a secure manner. Ideally, such a solution:

- could be implemented on a portable electronic device such as a mobile phone, tablet computing device, laptop, PDA etc, or on a desktop computer or fixed device;
- 10 • would enable PIN-based authentication to be performed on any suitably arranged device having some computing capabilities;
- would require the user to enter his PIN using the same digits as his stored PIN and in the same order (rather than requiring the user to enter an 'encoded' or somehow disguised/translated version of his PIN);
- 15 • would be easy and intuitive to use;
- would not require the user's machine to have access to the user's 'real' PIN, or any knowledge of how to calculate it
- would not need to execute any conversion or encoding algorithm (which carries with it a time and processing overhead, and can be used to discern the user's PIN).

20

Such an improved solution has now been devised which provides at least these advantages.

Thus, in accordance with the present invention there is provided a method and system as claimed in its various embodiments herein.

25

According to a first aspect of the invention, there may be provided a computer-implemented verification method comprising the step of:

enabling a user to input an identifier into an electronic device having:

- i) a screen; and
 - 30 ii) a keypad operable within a keypad zone of the screen;
- by operating at least one key of the keypad via an image of at least part of a scrambled keypad which is displayed at least partially within the keypad zone.

The image may be referred to as a 'scrambled keypad image' for ease of reference.

The keypad is operable in that has the functionality expected of a keypad by a person
5 skilled in the art. The skilled person would understand the term 'keypad' to mean an
electronic or mechanical grid of keys, each having at least one indicia associated with it,
which, when selected by a user, causes the associated indicia to be inputted into a device or
system for storage and/or processing. In the context of the present invention, the keypad is
an electronic version of a keypad. It may be thought of as a 'virtual' keypad in that it is a
10 software emulation of a mechanical keypad. It provides all the functionality of a
mechanical keypad, comprising labelled keys which the user can select to provide input to
a computer-based system.

The keypad may be generated on or by the electronic device. It may be generated by a
15 procedure call. The procedure may be provided within a library supplied by the
manufacturer of the device.

By contrast, the scrambled keypad image is a representation of a keypad. The
representation may comprise a representation of a whole keypad or at least part of a
20 keypad. It may depict (represent, illustrate) one or more 'keys'. The image may be
electronically formed. It may be a graphical image, an optical image, a video or some
other form of visual representation. It may be formed or stored in digital format in an
electronic file.

25 This provides the advantage that the layout of the 'keys' in the representation may not be
easily read by an unauthorised party who might intercept the representation during
transmission or while it is displayed on the electronic device.

The scrambled keypad image is not a keypad *per se* because it is devoid of any
30 functionality. It is merely a representation of a grid of keys. Touching, clicking on or
otherwise selecting any 'key' depicted in the image does not, in and of itself, produce any
effect or generate an input.

-10-

However, it should be noted that the scrambled keypad image may sometimes be referred to as a 'keypad' 'scrambled keypad' or an 'overlying keypad' purely for ease of reference because in use it *appears* to function as a keypad. Areas of the image may be referred to as
5 'keys', again only for ease of reference because this is what the user appears to see and use. However, it should be remembered that this is not actually the case, and that the image is not a keypad in reality.

The invention may enable the user to enter his identifier via the same device component
10 that is used to display the scrambled keypad image (the screen). Phrased another way, the screen may serve as both the output (display) device for the scrambled keypad image and the input device via which the user's identifier may be entered. This contrasts with any prior art disclosure wherein the keypad is displayed on one device component (e.g. screen) and the user's input is received via another device component (e.g. keyboard).

15 An advantage of this feature is that it may enable the user's input from the image to be mapped to the electronic keypad which may be at least partially hidden from the user's view such that the user's input is automatically encoded upon entry by the user. The input is automatically encoded in the sense that the electronic device may not need to convert,
20 encode or in any way process the user's input. The keypad may be generated by a procedure call executed on the electronic device. The operable, electronic keypad may be referred to as a 'reference' or 'underlying' keypad for ease of reference.

Preferably, the user's operation of the keypad key via the image generates an encoded
25 version of the user's intended input. Preferably, the image is displayed within the keypad zone such that as the user touches, clicks on or otherwise identifies a location within the image, an operable keypad key at that location is activated to provide an encoded version of the user's input.

30 Thus, the user's identifier is input via the image. The user may select a portion of the image in order to enter the identifier. The image portion may resemble or depict a keypad key. Thus, the user may operate the keypad through the image.

-11-

Preferably, the image functions as a mask or cover superimposed over the keypad such that when the user touches, clicks on or otherwise identifies a location within the image it operates or activates the keypad key positioned at that location within the keypad zone.

5

Preferably, the keypad zone and/or the image remains in a fixed position on the screen during input of the user's identifier. This differentiates the invention from those known systems wherein the keys or entire keypad move on the screen during the verification process. As the image of the present invention remains in a fixed location, this provides a
10 solution which is easier to use and requires less processing by the electronic device.

Thus, in one sense the invention may be viewed as enabling a scrambled keypad image to be 'superimposed' over an 'underlying' keypad such that when the user enters his input via the overlaid scrambled keypad image it is encoded in accordance with the layout of the
15 underlying (preferably unseen) keypad.

The 'underlying' keypad may be viewed as an object generated and residing in the device's volatile memory at run-time to provide a model of a conventional mechanical keypad.

20 Thus, the invention provides the advantage that the user's 'real' identifier is never stored within the device and is not transmitted for verification. Therefore, the user's identifier cannot be derived by any potential interceptor without knowledge of the mapping between the overlaid image and underlying, functional keypad.

25 Preferably, the mapping between the overlaid image and underlying keypad is not stored in the electronic device, or derivable by the electronic device. The mapping (or correlation) between the positions of the two sets of 'keys' may be stored on a server remote from the electronic device.

30 Preferably, the scrambled keypad image may be sent from a remotely located computer-based resource to the electronic device. The resource may be a server. Thus, the scrambled keypad image may not be generated on the electronic device. A version of the

-12-

scrambled keypad image may be stored on the server. The version may be a record of the order of the symbols (“keys”) in the scrambled keypad image.

The keypad zone may be a defined area or portion of the screen. Thus, the keypad zone
5 may occupy the entire screen area or a portion of the screen. The scrambled keypad image may be displayed such that it covers the keypad zone completely, exactly or partially. Preferably, the underlying keypad is at least partially hidden from view so that the user is not able to see at least some of the keys of the keypad.

10 The identifier may be a Personal Identification Code. It may be a PIN (Personal Identification Number). It may comprise any number, type or combination of symbols or indicia (as explained above). The identifier may have been pre-selected by the user prior to executing the presently claimed method. The identifier may be stored remotely from the electronic device e.g. on a server. The scrambled keypad image and/or keypad may
15 comprise numeric digits, alphabetical characters, punctuation, symbols or any other indicia, or a combination thereof. One or more symbols may be associated with each key.

Preferably, the user may be able to select a plurality of “keys” in the scrambled keypad image to input an identifier comprising more than one symbol.

20

The scrambled keypad image may be scrambled with respect to a reference keypad. The keypad image may depict a block or grid comprising a plurality of adjacent keys. It may be ‘scrambled’ in the sense that the symbols on the “keys” are not in sequential order and/or not in the order which one would expect, perhaps with reference to the reference
25 keypad. The scrambling may be in accordance with a random generation process, or a process that approximates to a random process. The reference keypad may be the keypad operable within the keypad zone, or a default keypad associated as standard with a make, model, type of electronic device.

30 Thus, the same indicia may be present in both the underlying keypad and the scrambled keypad image but they are provided in different positions. Put yet another way, the order of the keys in the reference keypad is different from that of the scrambled image. The

-13-

scrambled keypad image may provide the same ‘look and feel’ as the default keypad associated with the electronic device, but with the “keys” in different relative positions.

The respective positions of one, some or all “key(s)” in the scrambled keypad image may
5 be different from the position of the same key(s) in the underlying keypad.

The user may operate the keys of the underlying keypad via the scrambled keypad image by interacting with the “keys” displayed on the screen. For example, the user’s input may be entered by the user touching the screen (with a finger or other device) or by selecting
10 the desired “key(s)” using a pointing device such as a mouse or tracker ball. Other selection methods may be used to similar effect, thus falling within the scope of the invention.

The position and/or dimensions of the keypad zone may be specified by a procedure or
15 method call.

Preferably, the keypad zone comprises a plurality of sub-zones or ‘hot spots’. The position of at least one ‘key’ in the scrambled keypad image and/or keypad may correspond to the position of a sub-zone such that there may be a mapping between the “keys” of the
20 scrambled keypad and the keys of the keypad and/or the plurality of sub-zones. It is desirable that the mapping is not derivable from or by the electronic device. The hotspots may underlie the keys of the scrambled keypad image.

The (underlying) keypad may be scrambled after each of the user’s key selections. Thus, a
25 different scrambled underlying keypad may be used for each keystroke of the user’s input.

Preferably, the scrambled keypad image is received by the electronic device from a computer-based resource (e.g. a server) located remotely from the electronic device. It may be sent to the electronic device from the server in respect to a request for an image,
30 the request being sent from the device to the server. The scrambled keypad image may be generated by the server.

-14-

Preferably, the scrambled keypad image is pre-generated. In one embodiment this may mean that it is generated prior to, not in response to, the request from the electronic device. The image may be generated prior to execution of the verification method.

- 5 The encoded version of the user's input (identifier) may be sent from the electronic device to a remote computer-based resource. This resource may be a server. Preferably, the server receives the encoded version of the user's input and processes it. The processing may provide a decoded version of the user's inputted identifier.
- 10 Thus, the user's 'real' identifier may not be transmitted. Only the encoded version may be transmitted, which may be meaningless to an unauthorised party who does not know the mapping between the the "keys" in the scrambled keypad image and the keys in the underlying keypad.
- 15 The decoding may be performed using a stored version or form of the scrambled keypad image. The stored version or form of the configuration of the keys may be a filename. The decoding step may provide a decoded version of the user's input. Thus, the user's 'real' identifier may be generated by translating each symbol in the encoded version into its corresponding counterpart in the scrambled keypad image.
- 20 The user's decoded input may be compared with a stored version of the identifier. The user's input may be deemed to be correct if the input matches the stored identifier.

Preferably, the method further comprises the steps:

- 25 generating a plurality of scrambled keypad images;
selecting one scrambled keypad image from the plurality; and
sending a copy of the selected scrambled keypad image to the electronic device.

The method may further comprise the step of:

- 30 removing at least one scrambled keypad image from the plurality prior to performing the selection.

-15-

The method may further comprise the step of:

removing the selected scrambled keypad image from the plurality after sending the copy to the electronic device.

5 The method may further comprise the step of:

removing from the plurality any scrambled keypad image which has at least one key in the same position as the same key in a reference keypad.

Preferably, the positions of the keys in the scrambled keypad image remain unchanged

10 relative to one another during input of the user's identifier. This is in contrast to prior art arrangements in which the position and/or order of the keys displayed to the user may scramble or rearrange or move on the screen after each of the user's key selections and/or after each verification session.

15 Preferably, the symbol of at least one key in the scrambled keypad image is at least partially obscured or obfuscated but remains readable to the user. This may have benefits in making the representation difficult to read using OCR software. This enhances the security of the system and method.

20 The electronic device may be a mobile telephone, a PC, a tablet computer, a laptop, a PDA, a card-reading terminal or other electronic device having a screen. The electronic device may be able to support a communications protocol such as TCP/IP, either over a wireless or fixed line, although other protocols may be supported, such as Bluetooth, RS232 etc.

25

The communication between the device (e.g. mobile phone) and the computer-based resource (e.g. server) may be via a fixed telecommunications line or via a mobile telecommunications/wifi etc. connection - essentially any IP-based device may be used.

30 The scrambled keypad image may be displayed via a web browser, or an application embedded within a browser, or a standalone software application, and/or an application

-16-

providing a graphical user interface to allow the user to interact with the scrambled keypad image.

It is preferred that the mapping correlation between the indicia positioning of the
5 scrambled keypad image and the underlying keypad is stored remotely from the device,
typically at the computer based resource remote from the device.

In order to enhance security, the scrambled keypad image may be renamed and/or
encrypted prior to being sent to the electronic device. This provides the benefit that 3rd
10 parties (such as malware) are prevented or at least impeded from intercepting and decoding
the identifier.

The method may further comprise the step of delivering an indicator to the user to confirm
that the scrambled keypad image has been provided by a legitimate source. The indicator
15 may be a 'watermark'. The indicator may be a textual message, image, video, sound,
vibration or other tactile indication. The indicator may have been chosen by the user.

Preferably, the scrambled keypad image is erased from the electronic device following the
user's input, or following a specified period of time.

20 A new (i.e. different) scrambled keypad image may be sent to the device if the user makes
a mistake when inputting the identifier.

Also in accordance with the invention there may be provided a computer-implemented
25 method for verifying a pre-stored Personal Identification Code (PIC), the method
comprising the steps:

- generating a representation of a keypad wherein the position of at least one indicia
in the representation is different from the position of the respective indicia in the
keypad;
- 30 - sending the representation to a remote device for presentation to a user to enable
the user to input a PIC using the representation;
- receiving an encoded version of the inputted PIC from the remote device;

-17-

- decoding the encoded version to provide a decoded version of the inputted PIC
- comparing the decoded version of the inputted PIC with the pre-stored PIC

According to a second aspect, there is provided a computer-implemented method for

5 verifying a pre-stored Personal Identification Code (PIC), the method comprising the steps:

- receiving a representation of a keypad from a remotely located computer-based resource, wherein the position of at least one indicia in the representation is different from the position of the respective indicia in the keypad;
- presenting the representation to a user to enable the user to input a PIC using the
- 10 representation;
- generating an encoded version of the inputted PIC;
- sending the encoded version of the inputted PIC to the computer-based resource for decoding such that the decoded version of the inputted PIC can be compared with the pre-stored PIC.

15

According to a further aspect, there is provided a computer-implemented method for verifying a pre-stored Personal Identification Code (PIC), the method comprising the steps:

- using a computer-based resource to generate a representation of a keypad wherein the position of at least one indicia in the representation is different from the
- 20 position of the respective indicia in the keypad;
- sending the representation to a remote device;
- presenting the representation to a user via the remote device to enable the user to input a PIC using the representation;
- sending an encoded version of the inputted PIC from the remote device to the
- 25 computer-based resource;
- using the computer-based resource to decode the encoded version to provide a decoded version of the inputted PIC and compare it with the pre-stored PIC

According to another aspect of the invention there is provided a computer-implemented

30 verification method comprising the step of:

enabling a user to input an identifier by selecting at least one key via a scrambled keypad

-18-

presented to the user within a keypad zone of a screen associated with an electronic device.

According to another aspect of the invention there is provided a computer-implemented system arranged and configured to perform any embodiment of the method described

5 above.

The benefits of the invention include:

- a reduction in the likelihood of fraud arising from CNP transactions;
- a significant reduction in the cost associated with such fraud;
- 10 - a shift in liability from the card issuer to the user in respect of fraudulent card usage;
- the convenience for the user of secure CNP transactions.

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

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

20 Figures 1 to 4 illustrate some examples of the various types of keypads that can be generated in accordance with the invention.

Figure 5 illustrates the production of a scrambled keypad representation according to an exemplary embodiment of the invention.

25

Figure 6 illustrates the Registration process in accordance with the invention.

Figure 7 illustrates an exemplary custom keypad database created for the registered device.

30 Figure 8 shows an illustrative transaction process in accordance with the invention;

-19-

Figures 9 and 10, illustrate an overview of an example secure transaction application process in accordance with an embodiment of the invention.

Figure 11 shows an illustrative 'standard' keypad in accordance with an embodiment the
5 invention.

Figures 12a, 12b and 12 c show examples of scrambled keypad images which are suitable for being superimposed over the standard keypad of Figure 11.

10 Figure 13 shows a scrambled keypad images being superimposed on top of the standard (reference) keypad of a device.

Figure 14a shows a standard numeric key pad as known in the prior art.

15 Figure 14b shows a numeric keypad on a mobile phone as known in the prior art.

Figure 15a shows a pre-generated keypad image prior to the application of a watermark.

Figure 15b shows the keypad image of figure 15a with the watermark provided in the
20 bottom left corner of the keypad zone.

Figure 15c shows the keypad image of Figure 15b but with the watermark in a different position (bottom left).

25 Figure 15d shows the keypad image of 15a with a photographic image used as a watermark in the background.

Figure 16a to Figure 16e show different scrambled keypad images generated from 4 different numeric sequences.

30

Figure 17 shows a scrambled keypad image having a combination of alphabetical and numeric keys.

-20-

Figure 18 shows three partial images which, when shown repeatedly in rapid succession, form an apparently static, recognisable image.

- 5 Figure 19 shows an example of how the invention may be implemented within a financial transaction processing system.

Turning to the Figures, an exemplary embodiment is now described in relation to use with a mobile phone. However, the invention may be used to perform PIN verification on a
10 variety of different types of device, assuming that the device has some processing capabilities and a screen for the display of a keypad.

The exemplary embodiment also relates to use in respect of financial transactions. One application for which the invention is suited is that of on-line banking. However, the
15 skilled addressee will readily understand that the invention may be employed in other settings and for non-financial purposes. It is not limited to business or commercial applications.

Importantly, the invention can be used in any situation where verification of an
20 individual's identity is required before allowing that individual to have access to some controlled resource. That controlled resource may be any type of resource. It may be funds sitting in a financial account. Equally, it could be a building, a computer system, a patient's medical records, a service and so on. For example, it may be used for the verification of a passcode on a door lock to establish authentication prior to allowing entry
25 to a building.

It is important to note that the financially-oriented application described below is only one purpose to which this invention may be put. It has been selected for exemplary purposes because chip and PIN verification is perhaps the most widely known use of code-based
30 verification and therefore most readily recognised by readers of this document. However, the skilled addressee will understand that the invention is not limited in respect of the environment or context in which the invention may ultimately be put to use.

It is also important to note that the invention does not constitute a means for performing a transaction *per se*. It is a verification tool useful for authenticating the identity of an individual who has requested access to a controlled resource. It does not dictate how that
5 access is performed after authorisation is established, neither does it dictate how any other operation or possible transaction is conducted following successful verification.

The exemplary embodiment described below essentially operates by creating an image of a scrambled version of a keypad (which may alternatively be called a 'PIN pad'). The
10 scrambled keypad image is sent for presentation or display on the target electronic device 1 for the user to view. In this example, the target device is a mobile phone 1, as shown in Figure 6.

The scrambled keypad image is arranged to resemble the standard, default keypad for the
15 device. Each brand and/or model of device typically has its own style of default keypad which might be different in layout, symbols, size, colour etc. from the default keypads associated with other devices. The default keypad is usually generated and displayed on the mobile phone by a procedure call, which specifies the format of the keypad for that device and where it is to be displayed on the screen. The default keypad is a grid which
20 occupies a specific area on the screen i.e. it is displayed at a specified location. It is a pre-defined area or portion (referred to herein as a 'keypad zone') within the phone's screen. The keypad zone is divided up into sub-zones wherein each sub-zone represents a key in the default key pad. Another way of saying this is to say that each sub-zone is associated with a particular symbol. The symbol for each key is displayed for the user to see on the
25 screen within the location of its respective sub-zone. Therefore, if the user selects (e.g. touches or clicks on) an area designated to a particular sub-zone, the symbol for that associated key is recorded. In this way, the keypad serves as a virtual version of a mechanical keypad, generated electronically by software, detecting the location of the user's input within a defined screen area and using that to generate the input data rather
30 than using physically pressable keys.

-22-

In such virtual keypads, each subzone is essentially a 'hotspot' on the screen, and a plurality of hotspots are combined adjacent one another to form a keypad. In the present example, the default keypad 2 of the phone is arranged as a 3x4 grid of keys, each key 4 having a symbol associated with it. In this case, the symbols include numeric digits. Each
5 key 4 is a 'hotspot' area of the screen, each hotspot being associated with a symbol in the virtual keypad.

An example of a well-known style of default keypad 2 used with smart phones is shown in figure 11. The default keypad 2 is generated on the target device 1 itself – it is not sent to
10 the device 1 from the remotely located server.

This standard keypad 2 is then 'overlaid' with the scrambled keypad image 3 which is sent to the phone and is displayed on the screen at the keypad zone. This superimposition is achieved by displaying the image of the scrambled keypad within the keypad display zone
15 such that the positions of the scrambled 'keys' correspond to the positions of the hotspots in the default keypad. The alignment of the two keypads is such that only the scrambled keypad image is seen by the user and the underlying, operable keypad is hidden, at least partially but preferably entirely, by the image. Therefore, as far as the user is concerned, there is only one keypad, which looks exactly like the keypad the user expects, except with
20 the keys in different positions relative to one another.

As the default keypad for the mobile phone is the 'norm' against which the scrambled keypad is referenced, it may be referred to as a 'reference keypad'.

25 Figures 12a, 12b and 12c show examples of keypad images 3 which are suitable for overlay on top of the standard keypad 2 of Figure 11.

The scrambled keypad is sent to the phone as an image. Alternatively, it could be sent as a video file, to be discussed in more detail further below. This picture, video or image 3 may
30 be referred to as a 'representation' because in one sense it represents a physical (depressible) keypad.

-23-

The scrambled keypad image 3 has been pre-generated (i.e. prior to the initialisation of the verification process). It is randomly selected from a set of pre-generated scrambled keypad representations and then sent over a telecommunications network to the handset (i.e. mobile phone) 1. The scrambled keypad image of figure 3 is a representation of the
5 default keypad layout 2. The difference between the default keypad 2 and the scrambled keypad image 3 is that the respective keys 4 are ordered differently. In other words, the same digits are present in each keypad but at least two are in different positions within the keypad grid.

10 This keypad representation 3 has been generated to have exactly the same dimensions as the default keypad so that it can perfectly superimpose it. Thus, the mobile phone user (customer) views only one seamless keypad. The user is unaware that there is an underlying keypad 2 which has been generated in the background, behind the one that he sees and uses for entering his input. The image is sent to the user's device together with
15 one or more instructions to invoke or call the necessary procedure for generating the underlying keypad.

The randomly-selected, scrambled keypad image 3 is effectively overlaid onto the phone's default keypad 2 so that when the user enters his PIN, a different result is generated within
20 the device other than that which the user intended to enter, or at least thought he was entering. This is achieved as a result of the relationship (mapping) between the differently positioned keys 4 in the two keypads 2, 3. The user touches the screen at a particular location to enter a digit shown in the overlying scrambled keypad image 3, but this is interpreted as being the digit in the underlying keypad 2 at that sub-zone. As the user
25 enters a subsequent input its corresponding, underlying symbol is concatenated to the previous input to construct a complete PIN.

In this way, an encoded version of the user's PIN is produced based upon the position of the hidden keys 4 which the user selects via the scrambled keypad representation 3. If the
30 user makes a mistake, a new (different) keypad representation 3 is sent to the device 1.

-24-

Thus, the PIN that the user thinks he is entering is not the PIN recorded by the software residing on the user's phone. The user's 'real' PIN is never stored on the insecure phone 1, and is not transmitted over any (insecure) network. Only the encoded version is stored, transmitted. The encoded version of the PIN may be encrypted prior to transmission to
5 further enhance security. Thus, any interceptor would be unable to decode, guess or re-translate the real PIN without knowing how the positions of the keys in each keypad map to one another.

In the present embodiment, the decoding process is handled by a component of the
10 invention which 'knows' the layout of the keys in both keypads and is, therefore, able to map the encoded digits back to their original counterparts, thus arriving back at the user's intended input. This deciphered PIN can then be compared against the user's previously stored PIN for verification purposes.

15 In the exemplary embodiment, the scrambled keypad image 3 is encrypted before it is sent to the phone 1. Upon arrival at the phone 1 it is loaded into a secure or protected portion of memory on the device 1 (or at least as protected as it can be). In other words, all of the usual security features are used by the invention as if the customer's real PIN has been entered (rather than a translated version). This provides another layer of security and
20 protection.

These aspects of the invention are now discussed in greater detail in relation to one way in which the invention can be put into use.

25 **Pin Pad Production**

The 'PIN Pad Production Program' 6 is responsible for generating all of the scrambled keypad images 3 used throughout the system. An overview of this aspect of the invention is shown in Figure 5.

30 If simply randomly scrambled keypads are used, there is a risk that one or more keys may not be positionally scrambled. This could resort in one or more keys of the users input PIN corresponding positionally on the standard and scrambled PIN. This is not ideal.

-25-

Consequently, during PIN pad (image) generation, scrambled key pad images that would have one or more keys positionally corresponding to the standard keypad are discarded. The PIN pad production is therefore preferably not purely random, but is subjected to a
5 selection process to select/discard according to a specific criteria.

The PIN pad (image) generation takes place in a secure environment, typically compliant with payment card industry data security standard.

- 10 The output resolution and file type must be initially set up before use on a particular target device 1 (in this case the type of mobile phone). This ensures that outputted images are generated to the optimum resolution for that device e.g. 256 x 184.

- A master 'Background Image' 7 is then selected which matches the resolution as set above,
15 and a 'Permutations File' 5 selected containing all the required permutations of digits (keys) for the final keypad images. In one implementation, this file 5 must be a comma separated text file with each permutation on a new line. However, a variety of implementations may be devised to the same effect. For example, each permutation could be separated by a # or *.

20

The 'Permutations File' 5 is then merged with the 'Background Image' 7 using the user's selection of Font Type, Size and Colour to produce the completed keypad image 3. The completed keypad image 3 is then optimized and reduced in size to be as small as possible for optimum transmission speed.

25

In addition to standard monochrome keypads as shown in figures 1, 5, 9 11, 12 and 13, the background image 7 may be manipulated. For example, the colour of the background and/or the default font type, size and colour can be altered so that an unlimited database of keypads may be generated for every type of screen and device.

30

In some embodiments, advertisements, educational messages or other content may be incorporated in the presented imagery.

-26-

These keypad images may employ special fonts or colours to enable any specific regional characters e.g. Arabic to be used, and also to ensure that the images cannot be read by unauthorised Optical Character Recognition programs (thus enhancing security).

5

Each keypad image that is produced is also given a unique filename and a master index is created for all keypad images that have been generated. When a scrambled keypad image is sent to the device, a copy of the filename of that image is temporarily stored. This filename contains the order of the keys within the keypad image. This enables the mapping between the scrambled keypad image and the reference keypad to be recorded.

10

For security purposes, the scrambled keypad image 3 is renamed before it is encrypted and sent to the remote device 1; this prevents malware or other unauthorised parties from possibly intercepting and decoding the PIN.

15

Figures 1 to 4 illustrate some examples of the various appearances that the scrambled keypad images 3 can be provided with in accordance with the invention.

20

By way of example, Figure 2 shows a scrambled keypad image 3 having a background of autumn leaves. This can be used by the retailer for seasonal variations or can be used for advertising purposes.

25

Figure 3 shows a black and white only image distorted so that it cannot be read by OCR software. The skilled addressee will be aware that such images require high resolution screens to display correctly.

30

Figure 4 shows a monochrome keypad image that has been modified for the Arabic alphabet. The skilled addressee will appreciate that this regional difference in the characters can also be combined with the other imagery techniques methods illustrated in figures 2 and 3.

-27-

On suitably powerful devices, a video overlay may be used instead of a static image to further decrease the potential that OCR software could be used to read the keypad. This feature could also be used for advertising purposes.

- 5 It is important that, in order to provide a necessary level of security, malware and unauthorised parties are not able to read the data contained in the scrambled keypad image displayed to the user. As described above, this is achieved by the invention by providing the scrambled keypad in a single image or picture format. While it is possible to OCR images on a microcomputer, mobile telephones do not have the capabilities to do this, and
10 it would be almost impossible for hidden malware to possess the required level of sophistication without attracting detection.

- This issue can, at least in part, be addressed by using random backgrounds and fonts which cannot be understood by OCR technologies. The problem could also be addressed by
15 delivering the keypad image as a video file. While video files do not lend themselves to being read by OCR technologies it is technically possible for a third party to 'grab' a single screen from a video file and read it.

- One solution which may be incorporated into various embodiments of the invention would
20 be to combine the two afore-mentioned systems into one. Thus, the scrambled keypad image is presented to the user in a plain format (ie non special fonts are used and the background is 'normal') but the file itself is a small video file which, when played, tricks the eye into thinking that the image is solid and static. In reality no single frame contains enough information for it to be reverse engineered back into understandable, useable
25 content.

- The system can be achieved in as little as 3 frames, each played quickly and in succession so as to appear static. An example is given in Figure 18. When combined into a video file the static word 'Licentia' is displayed but the individual images are unreadable by an OCR
30 package.

Registration Process

-28-

This aspect of the invention is illustrated in Figure 6.

In certain embodiments, a device 1 must be registered before it can be used with the system of the present invention and a small application 8 downloaded to the target device

- 5 1. If the device being used is a mobile phone 1 then the update process can occur 'Over The Air' automatically; if the device is a fixed terminal then the software 8 may be downloaded over a fixed line, although it may alternatively be built into the device at the time of manufacture and simply updated if required.

- 10 To register a mobile phone 1 with the system the user would need to undertake a registration process comprising the following steps:

1. Logo onto registration service 9 via a web-based interface (e.g. web site) 10
2. Enter their personal details i.e. Name, Address, Postcode (ZIP), Phone Make Model, Email address, Mobile Phone Number

- 15 The nature and type of data required may be stipulated by the system operator and vary from country to country depending on the application with which the system is being used. Furthermore, registration data may already be held by the operator as the customer may be an existing client and therefore only the application may need to be pushed to the device.

- 20 3. A link is then sent to the mobile handset 1 for the user to follow or the application 8 is simply 'pushed' down to the handset.

- When run for the first time, the application 8 sets up the device 1 and downloads any additional data which may be required, such as encryption keys etc. A custom keypad image database is also created on the server for the registered device (as
- 25 shown in Figure 7).

To register onto the system with a fixed device the user would complete a similar process as follows:

1. Logo onto registration service 9 via a web-based interface 10
- 30 2. Enter their personal details i.e. Name, Address, Postcode (ZIP), Phone Make Model, Email address

-29-

As above for the mobile phone, the required data would be dictated by the system operator.

3. The device then connects to the server either via a fixed line or wireless and if required updates the internal application. Any additional data that is required, such as encryption keys etc., is downloaded. A custom keypad image database is also created on the server for the registered device (see Figure 7)

Consider Figure 7. For both scenarios outlined above, for each device that is registered onto the system a custom database (or index) 13 of keypad images is created from the Master Database 11. The Master Database consists of keypad images that have been generated specifically for the user's registered model of device to ensure optimal display. This database (or Index) 11 is then randomized 12 to ensure that no two devices have the same order of scrambled keypad images i.e. keypad ref 'AXF015689.gif' may be in location 65894 for one device but in position 125948 on another. Again, this enhances security.

It should be noted that in certain embodiments user registration may not be a requirement. This may be the case where the software is integrated into a 3rd party application. In such embodiments, the required registration method may have been put in place by the third party.

Transaction Process

This aspect of the invention is illustrated in Figure 8.

- Upon successful registration of the user and device, transactions can be performed. An authentication (PIN request) can be initiated by several methods depending on the manner in which the system has been integrated with 3rd party applications.

Typically integration occurs with 3rd parties who:

- a. Manufacture card swipe or chip reading devices that are attached to the mobile device, or

-30-

- b. Push financial information and subsequent payment request down to the handset
i.e. toll road applications; or
- c. Provide websites which require secure PIN entry to gain access to information
when used in applications such as online banking access.

5

However, the invention is not intended to be limited in this regard and the nature of service or resources provided by the 3rd party is not a limiting feature of the invention.

In all cases described above there is a common trigger for the PIN application to load and
10 perform the subsequent PIN entry process.

Once a request for an image has been received by the server (which may be referred to as the 'computer-based resource') the incoming device 1 is identified and authenticated and, if successful, the next keypad image from the device's 'Index' 13 is encrypted and
15 transmitted to the device 1. The keypad images are sent sequentially as per the devices 'index 2' as shown in item 13 of Figure 7 (in order from top to bottom) and are not reused.

Once the encrypted keypad image 3 is received by the device 1 it is decrypted and passed to the 'Secure Terminal Application'.
20

Secure Terminal Application

This aspect of the invention is illustrated in Figure 9 and Figure 10.

The 'Secure Terminal Application' is the program that resides on the target device/phone 1
25 or the fixed terminal and is responsible for the secure input and transmission of the user's inputted PIN back to the server.

As described above, a keypad 2 is created on the device in a 3x4 grid. Each hotspot is assigned a numerical character. The application then 'overlays' this reference keypad 2
30 with the randomised keypad representation 3 that has been pre-generated and sent down to the handset 1. This scrambled keypad representation 3 has been generated to exactly the same dimensions as the keypad 2 underneath and perfectly overlays it, as described above.

-31-

Thus, when the user enters their PIN number 14 using the scrambled representation 3, a different, encoded output is generated. In the example below, if the user's PIN was '6725' then the output from the keypad would be '0476'. It is the keypad output of '0476' that is
5 encrypted and sent back to the server's 'Decryption Engine'.

Once the keypad has been pressed four times the scrambled keypad image 3 is securely wiped using a secure deletion algorithm from the protected memory where it resides.

10 **The Decryption Engine**

Once the central server ('computer-based resource') receives the incoming encoded and encrypted PIN from the handset 1 it must be converted back into the original user PIN.

This is done by the 'Decryption Engine' which is held on a separate secure server solely
15 for this purpose. As described earlier, when the device 1 identifies itself to the server and requests a keypad image 3 the unique filename for the keypad image that was sent to the device 1 is temporarily stored. This filename contains the order of the keys within the keypad i.e. for the keypad image shown in figure 9 the filename would be '0347152986'. This enables the mapping between the scrambled keypad image and the reference keypad
20 to be recorded. For security purposes, the scrambled keypad image 3 is renamed before it is encrypted and sent to the remote device 1.

When the encrypted PIN arrives the message is firstly decrypted using the shared key used for the handset/device (this may be Triple DES or Public Private Key, or whatever is
25 deemed appropriate during development according to the handset).

Once the message has been decrypted the encoded PIN that was generated by the user input must be decrypted. To do this the filename of the keypad image that was sent is copied into a temporary array and then for each number that was generated by the user
30 input the number in the corresponding array position is substituted, thus revealing the actual PIN number.

-32-

So for the example above where the user's PIN was 6725, the handset generated and transmitted an encrypted PIN of 0476.

Now when the filename of the keypad image that was sent is copied into the array

5 '0347152986' we get the following:

Array Position	1	2	3	4	5	6	7	8	9	0
Filename Character	0	3	4	7	1	5	2	9	8	6

For each number in the generated PIN the 'Array Position' is located and the corresponding 'Filename Character' is substituted.

10

First Digit of PIN = 0 (GOTO array position 0); First digit of user's PIN number = 6

Array Position	1	2	3	4	5	6	7	8	9	0
Filename Character	0	3	4	7	1	5	2	9	8	6

Second Digit of PIN = 4 (GOTO array position 4) Second digit of users PIN number = 7

Array Position	1	2	3	4	5	6	7	8	9	0
Filename Character	0	3	4	7	1	5	2	9	8	6

15 Third Digit of PIN = 7 (GOTO array position 7) Second digit of users PIN number = 2

Array Position	1	2	3	4	5	6	7	8	9	0
Filename Character	0	3	4	7	1	5	2	9	8	6

Forth Digit of PIN = 6 (GOTO array position 6) Second digit of users PIN number = 5

Array Position	1	2	3	4	5	6	7	8	9	0
Filename Character	0	3	4	7	1	5	2	9	8	6

After the decryption process has been completed the user's 'real' input of 6725 is revealed.

20 This PIN number 6725 is then encrypted using standard banking encryption and passed to the Acquirer or banking partner for processing. It should be noted that this is only further encrypted and passed to the acquirer in embodiments relating to a financial transaction.

-33-

The data may or may not be further encrypted depending upon the nature and requires of the specific application.

The array is then securely erased to ensure security, along with any other temporary data.

5

It should be noted that in certain alternative embodiments, 12 smaller key pictures (one for each number or hotspot) may be provided. The phone or other device may be arranged to select a random number and rearrange the individual pictures into a 3x4 array (and thus making up a virtual keypad on demand). However, such embodiments present potential security loopholes and may provide several access points for malware to obtain the user's PIN (as the handset/device would have to transmit the random number and thus the order of the PIN pad back to the server). Therefore, such an embodiment is suitable for applications where required security levels are somewhat relaxed.

15 It should also be noted that although the invention has been described above in respect of a mobile phone having a touch screen, other embodiments may comprise a different type of device. For example, in another embodiment the device could be a personal computer, or a laptop, or a tablet computer. The embodiment would function essentially as described above except that as general purpose computing devices, such as PCs, do not typically
20 comprise a standard procedure call for generating a keypad as mobile phones do, the keypad zone and hotspots are specified by a purpose-built software component executing on the device. The software specifies the portion of the screen which makes up the keypad zone, and the locations of the sub-zones (keys) and their associated symbols within the keypad zone. The scrambled keypad image is displayed at that location to provide the
25 superimposition technique described above. The underlying keypad is generated using the same (or substantially the same) procedure call used by the smart phone implementation.

In another embodiment, a terminal could be provided which resembles the known card-reading terminals used in retail environments. The terminal may comprise a touch screen
30 and comprise internal components replicating those of a mobile telephone. Thus, the terminal can receive and send data as a phone can, and the terminal can function is

-34-

accordance with the invention as described above in with reference to the target device being a mobile phone.

Thus, the invention can be configured for use with a variety of computing-related devices
5 to equal effect.

In addition, the invention can be configured to include various features which further enhance the security of the user's data.

10 **Watermarking**

For example, so-called 'man in the middle attacks' are a known problem. This can be addressed in the present invention using a 'watermark' feature to demonstrate to the user (i.e. a retailer or possibly the end customer) that the input device is communicating with a legitimate party (e.g. the appropriate bank) and therefore that the scrambled keypad image
15 has been sent by that legitimate party and not an imposter.

Such a feature may be implemented in a variety of ways. For example, when a retailer registers to use the system they choose and store a secret indicator (word, phrase, number, name, image etc.) that only they and the trusted party knows. Then, when a transaction is
20 required the following process is performed:

1. the consumer's card is read
2. The transaction amount is entered
3. the pin entry screen is displayed on the terminal

25 When the PIN entry screen is displayed the merchant must physically check that the pre-selected secret word etc that they registered is displayed on the screen before handing the terminal to the customer for their PIN entry. This is essentially the same principle which is employed in ssl technology wherein one looks for the small yellow lock icon as confirmation of the site's legitimacy.

30

By doing this, the responsibility is placed onto the merchant to ensure that the device is talking securely to a legitimate party. If a different indicator (watermark) is displayed

-35-

from that which the merchant expects, or no indicator is shown at all, it can be assumed that the process has been compromised.

This watermark may stay on the screen for duration of the PIN entry by the consumer.

- 5 However, it is preferable that it is only displayed for a short period of time (e.g. the region of a few seconds) and then disappears before it may be seen by any other person, such as the customer. If the watermark is seen by another person, this could allow them to perform a man in the middle attack. Figure 15a shows a pre-generated pin pad picture that is blank. The system creates a new pin pad picture to include the user's secret word 'jellybean'
- 10 which is then encrypted and sent to the device. This is shown in Figure 15b.

- Upon registration the user may also choose where to have the watermark displayed e.g. right, left, centre, top etc. A keypad image having the watermark in the bottom left corner is shown in Figure 15c. In alternative versions, a text colour or font style, or size may also
- 15 be chosen.

- Moreover, the watermark does not have to be in textual form. In some embodiments, the user may upload a photograph or other file (for example, a family photo or a photo of the shop etc.) so that this picture is displayed in the background. This is illustrated in Figure
- 20 15d.

- This watermarking feature is suitable for employment with all embodiments of the invention, irrespective of the context in which the invention is used or the nature of the device used to display the keypad (e.g. online through a browser, via a terminal arranged
- 25 for use with the invention, or a mobile phone etc.)

Additional PinPad Encryption

- In order to further enhance the security of the system, the invention may employ one or more techniques for making it more difficult for an unauthorised party to figure out,
- 30 discern or calculate the mapping between the displayed keypad image (i.e. the one that the user uses to enter his PIN) and the underlying keypad.

-36-

For example, if the user has selected a PIN which contains the same digit more than once (e.g. 1223) this may make it easier to compute the correlation between the input and the 'underlying' keypad.

- 5 One possible approach to overcoming this could be to create more than one underlying keypad. For example, a virtual keypad could be generated for each key press. An example is given below.

Figure 16a shows a scrambled keypad image, and Figure 16b shows an 'underlying' keypad. If the user's PIN is 1111 then the encoded PIN sent back to the server would be 9999. This provides a potential hacker with a starting point for an attempt at calculating or guessing the user's PIN.

However, if 4 different 'underlying' keypads are used instead of one, this problem is overcome. Thus, a sequence of digits can be sent to the target device (e.g. terminal, phone, PC) and the sequence is used by the target device to form the keypad. For the keypad in Figure 16b, the sequence would be. 3156790482. Using this approach, it is possible to generate a new keypad for each required key press.

20 Thus, the top pin pad as per Figure 16a is sent to the target device as an image, in accordance with the description set out above. Then, 4 numeric sequences are sent for the creation of the underlying keypad e.g. 3156790482, 0746189352, 0347156289, 2581673904. This produces the keypads shown in figures 16b to 16e.

25 Suppose now that the user's input is 1111. Instead of 9999 being produced, the code 9857 is produced and sent back to the server for decryption. As the server 'knows' which scrambled keypad image was sent, and which sequences of digits, the resulting encoded PIN appears to be much more random and is therefore much harder to decipher by an interceptor. The decryption process at the server end remains as set out above.

30

Moreover, in order to enhance security further it is possible to use combinations of other characters in the generation of the keypads, not just characters. For example, the sequence Jg6KrBjoJ6 could be sent. This would generate the underlying keypad shown in figure 17.

-37-

In such an embodiment, the use of randomly generated strings of characters in the bottom keypad reduces the need to 'filter' the underlying keypads (as described above) to remove potentially unsuitable keypads which might provide an attacker with a possible starting point for an attack.

However in a preferred embodiment only 1.6m scrambled ('top') keypad images are used rather than the possible 3.6m and a check is still performed to ensure that no mapping is the same ie. 1=1 between the superimposed and the underlying keypads.

System level architecture

Figure 19 illustrates one manner in which the invention may be implemented into a transaction system.

Figure 19 includes the following system components, or modules.

Device app: an app that runs on a terminal or mobile phone to manage user interaction and technical process flow including initiating a payment transaction, interacting with card reader, requesting an oPinPad (i.e. scrambled keypad image), encrypting the entered oPin and sending the transaction online for authorization.

OPinPad Management Module: a stand-alone application module that runs in a central secure data center on a dedicated server. It holds a database of all oPinPad TIF images and manages distribution of the oPinPad TIFs on demand.

Auth Client: a stand-alone application module that runs in a central secure data center, possibly on the same server as the oPinPad Management Module (or, in some embodiments on its own dedicated server). It receives the message from the Device and prepares it to be sent to the Payments Switch for Authorisation.

HPSAM Appliance: a stand-alone application module that runs in central secure data centre on a dedicated server. In some embodiments the server may be security hardened.

-38-

In figure 19, the following terminology is used:

- Device: Payment Terminal or Mobile Phone where payment transaction is taking place
- 5 • oPin: “Obfuscated PIN” – the encoded PIN which is generated by the keys of the underlying Device keypad; this is not the actual cardholder’s PIN
- Real Pin: The real PIN associated with the consumer’s card that would be ‘swapped’ for the oPin before being verified by the card issuer
- 10 • oPinPad: Obfuscated Pin Pad (i.e. the scrambled keypad image)– the TIF image which is presented to the card holder to enter their PIN and having ‘keys’ in scrambled positions relative to the underlying Device keypad
- oPinPad Array: Array to be used for mapping the oPin with the Real Pin, as described above
- HPSAM: Hosted Payment Security Access Module
- 15 • HSM: Hardware Security Module
- Card Reader: The terminal/mobile device which contains or is connected to a Card Reader which retrieves payment card details from the consumer
- Tag: Unique identification number assigned to the oPinPad to assist with later processing
- 20 • ZMK: Zone Master Key.

Referring to the numeric references in Figure 19, the process flow of the illustrative system is as follows:

0	The device initiates a payment transaction and captures the Amount (from the user interface) and Card Details (from the Card Reader). Sensitive data from the Card Reader is encrypted before getting to the App. The App goes online and requests an oPinPad from the server. If possible the oPinPad would be requested at the same time as the card details are retrieved from the Card Reader.
1	The oPinPad Management Module retrieves an oPinPad (i.e. scrambled keypad image) from a database and assigns it with a Tag. The oPinPad TIF and the Tag (unique id) are sent back to the device.
2	The oPinPad Array is sent to the HPSAM along with the Tag (unique id). All traces of the Tag/Array combination are deleted from the oPin Management Module (in particular from memory).

3	The Device App displays the oPinPad TIF (scrambled keypad) image on the device and gathers the oPin as described above; the oPin is immediately encrypted using a field encryption method (such as DUKPT). The whole authorization message is then sent to the Auth Client for payments authorization (this message includes the Amount, the encrypted card details and the encrypted oPin).
4	The Auth Client gathers the transaction details and passes it on to the Payments Switch.
5	The Payments Switch intercepts the transaction during standard routing processing so that the oPin can be replaced with the Real Pin. This is done by sending the oPin with the Tag to the HPSAM.
6	Using the Tag, the HPSAM retrieves the oPinPad Array and uses it to map the oPin to the Real Pin. The Real Pin is immediately encrypted using 3DES and a ZMK which is aligned with the Payments Switch.
7	The Real Pin is sent back to the Payments Switch as a PinBlock and is added to the transaction to make an industry standard Online Pin payments authorization message (such as, for instance, an ATM message).
8	The Real Pin block is translated using an industry standard HSM such that the encrypted Pin can be handled by the receiving institution (Acquirer, Processor, Issuer).

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 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 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 computer-implemented verification method comprising the step of:
enabling a user to input an identifier into an electronic device having:
 - 5 i) screen; and
 - ii) an operable keypad provided within a keypad zone of the screen, the keypad generated at run time and comprising a plurality of keys, each key having at least one indicia associated with it which, when operated by the user, causes the associated indicia to be inputted to the device;
- 10 by operating at least one key of the keypad via an image of at least part of a scrambled keypad which is displayed at least partially within the keypad zone, and which functions as a cover superimposed over the keypad such that when the user identifies a location within the image it operates the keypad key positioned at that location within the keypad zone to provide an encoded version of the user's input.
- 15 2. A method according to any preceding claim wherein the image is electronically formed, including a graphical image, an optical image, a video or some other form of visual representation.
- 20 3. A method according to any preceding claim wherein the keypad zone is a defined area or portion of the screen which covers the entire screen or a portion thereof.
4. A method according to any preceding claim wherein the image is displayed such that it appears to the user that the image is an operable keypad with keys in a scrambled
- 25 order or configuration with respect to the keypad of the electronic device.
5. A method according to any preceding claim wherein the keypad zone is a portion of the screen which is designated, prior to the user inputting the identifier, as a keypad display area.
- 30 6. A method according to any preceding claim wherein the keypad zone and/or the image remains in a fixed position on the screen during input of the user's identifier.

7. A method according to any preceding claim wherein the identifier is a Personal Identification Code or Personal Identification Number.
- 5 8. A method according to any preceding claim wherein the image represents or depicts a scrambled keypad having at least one key which is positionally re-ordered or reconfigured relative to the layout of the keys in the keypad.
9. A method according to claim 8 wherein the all of the keys depicted in the image are
10 repositioned or re-ordered relative to the keys in the keypad.
10. A method according to any preceding claim wherein the user is enabled to input the identifier by interaction with the screen, such as by touching a portion of the screen and/or selecting an area of the screen using a pointing device such as a mouse or
15 tracker ball.
11. A method according to any preceding claim and further comprising the step of:
sending the image to the electronic device from a remotely located computer-based
resource.
20
12. A method according to any preceding claim wherein the keypad zone comprises a plurality of sub-zones or 'hot spots', each sub-zone corresponding to a keypad key.
13. A method according to claim 12 wherein the image of the scrambled keypad is
25 presented to the user such that the position of at least one key depicted in the image corresponds to the position of a sub-zone, thus providing a mapping between the keys of the scrambled keypad depicted in the image and the plurality of sub-zones.
14. A method according to any preceding claim wherein the configuration or order of the
30 keys in the keypad is altered after at least part of the user's identifier has been inputted.

15. A method according to any preceding claim wherein an encoded version of the user's identifier is constructed within the electronic device from a plurality of keystrokes activated on the keypad in response to a click, touch or other indication made by the user in respect of the image on the screen.
- 5
16. A method according to any preceding claim wherein the identifier inputted into the device is sent from the electronic device to a remote computer-based resource.
17. A method according to claim 16 wherein the remote computer-based resource receives the user's identifier and processes it.
- 10
18. A method according to claim 17 wherein the identifier is processed using a stored form or version of the configuration of the keys depicted in the image of the scrambled keypad.
- 15
19. A method according to claim 18 wherein the stored form or version of the configuration of the keys is a filename.
20. A method according to claim 19 wherein processing involves using the stored form or version of the configuration of the keys to provide a decoded version of the user's inputted identifier.
- 20
21. A method according to claims 18 to 20 wherein the processed identifier is compared with a stored version of the user's identifier, and the user's input is deemed to be verified if the processed identifier matches the stored version of the identifier.
- 25
22. A method according any preceding claim wherein the image displayed on the device is selected from a plurality of images of scrambled keypads, preferably wherein the plurality is filtered in some manner prior to selecting the image, such as filtering the plurality to ensure that no image in the plurality depicts any keys which are in the same position as the corresponding key in the keypad.
- 30

23. A method according to any preceding claim and further comprising the steps:
generating a plurality of images of scrambled keypads;
selecting one image from the plurality; and
sending a copy of the selected image to the electronic device.
- 5
24. A method according to claim 23 and further comprising the step of:
removing at least one image from the plurality prior to performing the selection.
25. A method according to claim 23 or 24 and further comprising the step of:
10 removing the selected image from the plurality after sending the copy to the electronic device.
26. A method according to claim 23 to 25 and further comprising the step of:
removing from the plurality any image which represents a scrambled keypad having at
15 least one key in the same position as the respective key in the keypad.
27. A method according to any preceding claim wherein the positions of the all keys
depicted in the image remain unchanged relative to one another during input of the
user's identifier.
- 20
28. A method according to any preceding claim wherein the image of the scrambled
keypad is received by the electronic device from a computer-based resource located
remotely from the electronic device.
- 25 29. A method according to any preceding claim wherein the symbol of at least one key in
the image of the scrambled keypad is at least partially obscured or obfuscated but
remains readable to the user.
- 30 30. A method according to any preceding claim wherein the electronic device is a mobile
telephone, a PC, a tablet computer, a laptop, a PDA, a card-reading terminal, or a
mobile phone within a housing such that it resembles a card-reading or ePOS device, or
some other electronic device having communications capabilities.

31. A method according to any preceding claim wherein the image is displayed via a web browser, or an application embedded within a browser, or a standalone software application, or an application providing a graphical user interface to allow the user to interact with the screen.
32. A method according to any preceding claim and further comprising the step of delivering an indicator to the user to confirm that the image of the scrambled keypad has been provided by a legitimate source.
33. A method according to claim 32 wherein the indicator is an audible indication, a visual indication, a textual message, image, video, sound, watermark, vibration or other tactile indication.
34. A method according to claim 32 or 33 wherein the indicator has been chosen by the user.
35. A method according to any preceding claim wherein the position of the keypad zone on the screen, and/or its dimensions, are specified by a procedure or method call.
36. A method according to any preceding claim, wherein the image is erased from the electronic device following the user's input, or following a specified period of time.
37. A method according to any preceding claim wherein the user's inputted identifier is verified so as to control access to a resource such as a financial resource, a device, a building, an electronic resource, a medical resource, an information or data resource, or a computer-based resource.
38. A method according to any preceding claim and further comprising the step of: sending the image to the electronic device from a remotely located computer-based resource; and

sending at least one instruction to the electronic device, said at least one instruction configured to generate the operable keypad upon execution by the device.

39. A computer-implemented method for verifying a pre-stored Personal Identification

5 Code (PIC), the method comprising the steps:

- generating an image of a keypad wherein the position of at least one indicia in the image is different from the position of the respective indicia in an operable keypad;
- sending the image to a remote device for presentation to a user to enable the user
10 to input a PIC by operating at least one key of the operable keypad via the image, wherein:
the keypad is generated on the remote device at run time and comprises a plurality of keys each key having at least one indicia associated with it which, when selected, causes the associated indicia to be inputted to an electronic device;
- 15 and
the image functions as a cover superimposed over the keypad such that when the user identifies a location within the image it operates the keypad key positioned at that location within the keypad zone to provide an encoded version of the user's input;
- 20 - receiving an encoded version of the inputted PIC from the remote device;
- decoding the encoded version to provide a decoded version of the inputted PIC
- comparing the decoded version of the inputted PIC with the pre-stored PIC

40. A computer-implemented method for verifying a pre-stored Personal Identification

25 Code (PIC), the method comprising the steps:

- generating an operable keypad on an electronic device at run time, the keypad comprising a plurality of keys each key having at least one indicia associated with it which, when selected, causes the associated indicia to be inputted to the device;
- receiving an image of the keypad from a remotely located computer-based
30 resource, wherein the position of at least one indicia in the image is different from the position of the respective indicia in the keypad;

- presenting the image to a user to enable the user to input a PIC into the electronic device by operating at least one key of the keypad via the image; wherein:
the image functions as a cover superimposed over the keypad such that when the user identifies a location within the image it operates the keypad key positioned at that location within the keypad zone to provide an encoded version of the user's input;
- generating an encoded version of the inputted PIC;
- sending the encoded version of the inputted PIC to the computer-based resource for decoding such that the decoded version of the inputted PIC can be compared with the pre-stored PIC.

41. A computer-implemented method for verifying a pre-stored Personal Identification Code (PIC), the method comprising the steps:

- generating an operable keypad on an electronic device at run time, the keypad comprising a plurality of keys each key having at least one indicia associated with it which, when selected, causes the associated indicia to be inputted to the device;
- using a computer-based resource to generate an image of the keypad wherein the position of at least one indicia in the image is different from the position of the respective indicia in the keypad;
- sending the image to the electronic device;
- presenting the image to a user via the electronic device to enable the user to input a PIC using the image; wherein:
the image functions as a cover superimposed over the keypad such that when the user identifies a location within the image it operates the keypad key positioned at that location within the keypad zone to provide an encoded version of the user's input;
- sending an encoded version of the inputted PIC from the electronic device to the computer-based resource;
- using the computer-based resource to decode the encoded version to provide a decoded version of the inputted PIC and compare it with the pre-stored PIC

42. A computer-implemented system arranged and configured to perform the method of any preceding claim.