A method for a receiver of an electronic message to authenticate an identity of a sender of the electronic message. The message contains a one-time security code in the form of a string of characters generated by selecting characters from a sender-side non-repeating pseudorandom string of characters. This is done by applying a user-specific PIN in the form of a first sequence of digits to the pseudorandom security string at the sender by sequentially selecting numerical positions in the sender-side pseudorandom string on the basis of the numbers in the user-specific PIN, taken in positional order, and returning the characters thereby selected from the sender-side pseudorandom string in sequence so as to form the one-time security code. Upon receipt of the message, the receiver correlates the characters in the one-time security code with characters in a receiver-side non-repeating pseudorandom string of characters, identical to the sender-side pseudorandom string, by considering the characters of the one-time security code in sequence and identifying a numerical position of each character of the one-time security code in the receiver-side pseudorandom array to thereby generate second sequence of digits. The identity of the sender is authenticated when the second sequence of digits matches the user-specific PIN.
METHOD AND SYSTEM FOR AUTHENTICATING MESSAGES

[0001] The present invention relates to a method and system for authenticating messages sent to a subscriber or user using the Short Messaging Service (SMS) or other protocols used in mobile telecommunications and related fields.

BACKGROUND

[0002] Various systems are known for conducting electronic transactions in a more or less secure manner over a telecommunications link or the like. One well known system is known as electronic funds transfer at point-of-sale (EFTPOS), in which a user is issued with a credit or debit card bearing a unique identification number, usually embossed on the card in human-readable form and also encoded on a machine-readable magnetic strip on the reverse of the card. For further identification purposes, the card typically includes space for a user permanently to include his or her signature. In use, when a user wishes to make a purchase in, for example, a retail store, he or she presents the debit or credit card to a store employee. The card is then swiped through a card reader, and information relating to the identity of the card, the identity of the retail store and the value of the goods or services being purchased is transmitted by way of a telephone connection to a remote computer server operated by the card issuer (normally a bank or suchlike). The remote computer server checks that the user’s card account contains sufficient funds or credit to cover the proposed transaction, checks that the user’s card account is currently operational (for example, to check that the card has not been reported stolen), and then issues a confirmation signal back to the card reader to indicate that the transaction may be authorised. The store employee must then obtain a specimen of the user’s signature and compare this with the signature on the reverse of the card so as to check the identity of the user. If the signatures appear to match, the store employee operates the card reader to complete the transaction, and the funds required to cover the transaction are then electronically transferred from the user’s card account to the retail store. If the signatures do not appear to match, then the store employee may request additional proof of identification before authorising the transaction, or may simply refuse the transaction and retain the user’s card, which may have been stolen, thereby preventing any unauthorised transfer of funds. This system is open to fraudulent abuse, since it is possible for a card to be stolen and for a thief to forge the signature of an authorised user.

[0003] In a development of this system, a card user may be issued with a personal identification number (PIN), which is usually a four digit code, and which is theoretically
known only to the user and to the card issuer. Instead of or in addition to providing a specimen of his or her signature at the point-of-sale, the card user is required to enter his or her PIN into the card reader, and this information is transmitted to the remote computer server together with the card and retail store identification data and data regarding the value of the transaction. By providing an extra identification check by way of the PIN, this system helps to prevent fraud by forgery of signatures, but is still not completely secure because the PIN does not change between transactions, and may therefore be intercepted together with card identification data when being transmitted between the card reader and the remote server. Furthermore, it is possible for a thief to observe a user entering his or her PIN into a card reader and to remember the PIN. If the thief is also able to obtain card identification details, for example from a discarded till receipt or through conspiracy with the store employee, it is a simple matter to produce a fake card including all the appropriate identification information for later fraudulent use, or even to rob the authorised card user of his or her card.

[0004] A number of attempts to solve the problem of identity verification are currently available and include Public Key Infrastructure (PKI), SMART Cards, and biometrics.

[0005] A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. PKI provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as 'digital certificates' which act like 'electronic passports' and bind the user's digital signature to his or her public key. The PKI approach is only applicable for Internet or other transactions that use a computer because the complexity of the software at the users' end of the transaction requires significant computing resources. The PKI approach is not well suited to high volume transaction processing because of this complexity.

[0006] Smart Cards are a response to the problem of credit/debit card fraud. Smart Cards are cards that have a microchip embedded within the card which enables personal details about the cardholder to be stored securely on the card, which can then be used to verify the identity of the person using the card. The Smart Card system relies upon there being a Smart Card reading apparatus at the point of sale. Currently, few high street merchants have invested in such equipment, and recent industry estimates expect a hybrid smart card/magnetic strip environment for the next 10-15 years. In addition, smaller or independent retailers find the cost of such equipment is a deterrent to uptake. Few Smart Card systems address the problem of "card not present" fraud such as e-commerce, m-commerce, interactive TV and telephone order unless the consumers invest in Smart Card readers for the home. Similarly, any Smart Card can be copied ("skimmed/clone") and
can subsequently be used fraudulently in card not present situations. Most major card
issuers have plans to roll out such Smart Cards within the next few years, although the
costs of the equipment, the cards themselves and the availability of the chips may delay
this process.

[0007] A number of companies are currently developing biometric solutions to the
problem of cardholder verification. The Biometric systems can use fingerprints, voice
recognition, retinal scans or tissue samples to positively identify the cardholder. Similar to
smart cards these biometric systems would require complex and costly equipment at the
point of sale and would not provide any protection against fraud in card not present
situations.

[0008] It is known from US 7,392,388 in the name of the present Applicant (the entire
content of which is hereby incorporated into the present application by way of reference) to
provide an identity verification system in which a user can identify himself to a bank or
merchant computer or the like by applying a relatively simple protocol to a challenge string
received from the bank or merchant computer by way of an SMS message, or a secure
website by way of a Hypertext Transfer Protocol Secure (HTTPS) connection, or an email
communication or the like. The user is in possession of a short numerical code, analogous
to a typical Personal Identification Number (PIN) commonly used as a security measure
together with a credit or debit card. This numerical code, which may be four digits in
length (although other lengths may be used), is known only to the user and to the bank or
card issuer. The user applies the numerical code to a pseudorandom security string
issued by the bank or card issuer, by selecting characters from the security string, on a
positional basis determined by each digit of the numerical code, taken in order. For
example, where a user numerical code is "2473", and the pseudorandom security string is
"396&ftly7d3GG9", the user would return "9&y6", with "9" being the second (2nd) character
in the security string, "&" being the fourth (4th) character, "y" being the seventh (7th)
character and "6" being the third (3rd) character.

[0009] As an alternative to selecting characters from a security string on a positional
basis by way of a numerical code, the user may do so on the basis of applying a secret
shape or pattern to an array of security digits (rather like a Cardan grille), although
computationally the method is similar to that described above.

[0010] A special advantage of the type of encryption disclosed in US 7,392,388 is that it
is relatively simple for a user to apply mentally, although an applet or small application
running on a mobile device owned by the user could also be used, while still being
reasonably secure. In particular, assuming sufficient redundancy in the pseudorandom
security string, it is not easy for a third party to deduce the user's PIN or numerical code,
even if both a pseudorandom security string and a returned response from the user are hijacked.

[0011] A growing problem is that of “phishing” or, where a fraudulent third party seeks to obtain security information from an individual by sending out communications purporting to be from that individual’s bank or credit card issuer. Some of these phishing or communications are quite sophisticated, and can look almost identical to authentic communications. Moreover, it is relatively trivial for a fraudulent third party, when sending an email, to spoof an authentic email address of an individual’s bank or credit card provider. By placing a fraudulent hypertext link in the email, the fraudster tries to lure the individual to a spoofed website where login and other security details are requested, the individual believing that he is responding to an authentic communication from his bank or card provider.

[0012] While there are various techniques available to reduce this risk on the Web, for example by flagging suspect spoofed sites in search engines, it is trickier to do this on the level of m-commerce, where mobile phones and SMS messaging are typically used for conducting transactions.

BRIEF SUMMARY OF THE DISCLOSURE

[0013] In accordance with a first aspect, there is provided a method for a receiver of an electronic message to authenticate an identity of a sender of the electronic message, wherein the message contains a one-time security code in the form of a string of characters generated by selecting characters from a sender-side non-repeating pseudorandom string of characters by applying a user-specific PIN in the form of a first sequence of digits to the pseudorandom security string at the sender by sequentially selecting numerical positions in the sender-side pseudorandom string on the basis of the numbers in the user-specific PIN, taken in positional order, and returning the characters thereby selected from the sender-side pseudorandom string in sequence so as to form the one-time security code, and wherein upon receipt of the message, the receiver correlates the characters in the one-time security code with characters in a receiver-side non-repeating pseudorandom string of characters, identical to the sender-side pseudorandom string, by considering the characters of the one-time security code in sequence and identifying a numerical position of each character of the one-time security code in the receiver-side pseudorandom array to thereby generate second sequence of digits, and wherein the identity of the sender is authenticated when the second sequence of digits matches the user-specific PIN.
[0014] In accordance with a second aspect, there is provided a system for a receiver of an electronic message to authenticate an identity of a sender of the electronic message, the system comprising a receiving device and a transmitting device that are operable to communicate electronically with each other; wherein the receiving device includes a memory containing at least one receiver-side non-repeating pseudorandom string of characters and the transmitting device includes a memory containing at least one transmitter-side non-repeating pseudorandom string of characters identical to the receiver-side pseudorandom string and a user-specific PIN in the form of a first sequence of digits; wherein the transmitter device further includes a processor to generate a one-time security code in the form of a sequence or pattern of characters by applying the user-specific PIN so as to sequentially select numerical positions in the sender-side pseudorandom string on the basis of the numbers in the user-specific PIN, taken in positional order, and returning the characters thereby selected from the sender-side pseudorandom string in sequence so as to form the one-time security code; wherein the transmitter is configured to transmit an electronic message including the one-time security code to the receiver; and wherein the receiver is configured, upon receipt of the message, to correlate the characters in the one-time security code with characters in the receiver-side pseudorandom string by considering the characters of the one-time security code in sequence and identifying a numerical position of each character of the one-time security code in the receiver-side pseudorandom array to thereby generate second sequence of digits; and wherein the identity of the sender is authenticated when the second sequence of digits matches the user-specific PIN.

[0015] The receiving device may be a mobile electronic communication device, such as a mobile phone, smart phone, laptop computer, netbook, personal digital assistant or pager. The receiver does not have to be a mobile device, and could simply be a communications-enabled computer.

[0016] The transmitting device may likewise be a mobile electronic communication device, or may be a non-mobile communications-enabled computer.

[0017] In an exemplary scenario, the receiving device is a mobile phone or smart phone or the like, and the transmitting device is part of a secure computer network at a financial or government institution, the method and system of the present invention being well-suited for to allow individuals to verify that electronic messages purportedly sent to them by their bank or a government body, are in fact authentic.

[0018] Where the receiving device is a mobile telephone or the like, the electronic message may be transmitted in the form of a text message under the short messaging service (SMS) protocol. Other well-known communications protocols, including email, may
be employed where appropriate, depending on the nature of the receiving communications device.

[0019] An important feature is that the transmitter-side and receiver-side non-repeating pseudorandom strings must be the same for each verification transaction. It is also preferred that a different pseudorandom security string is used for each verification transaction. This can be achieved by way of the transmitter and the receiver each running identical secure pseudorandom string generating algorithms in synchronism with each other. This type of technology is known, for example, from remote control automobile locking systems. Alternatively, the memories of the receiver and the transmitter may each contain identical sets of pseudorandom strings, and may be configured to step through these strings for sequential verification transactions. The transmitter may also be configured to generate a new pseudorandom string after each verification transaction and then to transmit this new pseudorandom string to the receiver in a separate transmission (i.e. not together with the one-time security code, since this would compromise the integrity of the encryption). This may be done individually, or batches of pseudorandom strings may be transmitted periodically to the receiver, without any one-time security codes, so that the receiver has a supply of pseudorandom strings that can be used in a predetermined sequence with matching transmitter-side pseudorandom security strings.

[0020] In order to avoid redundancy errors, the pseudorandom security strings must be made up of non-repeating characters. Accordingly, where decimal numbers are used, the pseudorandom security string can be a maximum of 10 characters in length if there are to be no repeated numbers. This provides 10! = (10x9x8x7x6x5x4x3x2x1) = 3,628,800 different possible pseudorandom strings, which gives a reasonable level of security. Security can be improved by including additional symbols, such as letters and other characters, allowing the string to be lengthened without any repetition of characters in the string.

[0021] As a simple example, suppose that the transmitter and the receiver are each in possession of the pseudorandom security string 3659814702, and the user PIN is 4856. The user PIN is securely known to the transmitter (e.g. a bank computer) and also by the user him/herself. At the transmitter, the user PIN is applied to the pseudorandom security string by selecting the 4th, 8th, 5th and 6th characters, namely 9, 7, 8 and 1 to generate a one-time security code of 9781. A message sent from the transmitter to the receiver contains this one-time security code. At the receiver, the one-time security code is applied to the pseudorandom string already in the receiver memory by looking for the position in the pseudorandom string of the characters 9, 7, 8 and 1 to recreate the user PIN of 4856,
thereby confirming the transaction. This process may be done manually where appropriate, or may be done automatically by a processor in the receiver.

[0022] It can be seen that the process works even when there is redundancy in the user PIN. For example, where the user PIN is 7887 in the above example, the one-time security code will be 4774, and applying this to the receiver-side pseudorandom string will regenerate the user PIN of 7887.

[0023] Where the pseudorandom strings include characters other than decimal numbers, for example 365gj78k2y, then a user PIN of 4856 will generate a one-time security code of gj7, and applying this back to the receiver-side pseudorandom string will return the user PIN of 4856.

[0024] Throughout the description and claims of this specification, the words “comprise” and “contain” and variations of them mean “including but not limited to”, and they are not intended to (and do not) exclude other moieties, additives, components, integers or steps. Throughout the description and claims of this specification, the singular encompasses the plural unless the context otherwise requires. In particular, where the indefinite article is used, the specification is to be understood as contemplating plurality as well as singularity, unless the context requires otherwise.

[0025] Features, integers, characteristics, compounds, chemical moieties or groups described in conjunction with a particular aspect, embodiment or example of the invention are to be understood to be applicable to any other aspect, embodiment or example described herein unless incompatible therewith. All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. The invention is not restricted to the details of any foregoing embodiments. The invention extends to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

[0026] The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.
CLAIMS:

1. A method for a receiver of an electronic message to authenticate an identity of a sender of the electronic message, wherein the message contains a one-time security code in the form of a string of characters generated by selecting characters from a sender-side non-repeating pseudorandom string of characters by applying a user-specific PIN in the form of a first sequence of digits to the pseudorandom security string at the sender by sequentially selecting numerical positions in the sender-side pseudorandom string on the basis of the numbers in the user-specific PIN, taken in positional order, and returning the characters thereby selected from the sender-side pseudorandom string in sequence so as to form the one-time security code, and wherein upon receipt of the message, the receiver correlates the characters in the one-time security code with characters in a receiver-side non-repeating pseudorandom string of characters, identical to the sender-side pseudorandom string, by considering the characters of the one-time security code in sequence and identifying a numerical position of each character of the one-time security code in the receiver-side pseudorandom array to thereby generate second sequence of digits, and wherein the identity of the sender is authenticated when the second sequence of digits matches the user-specific PIN.

2. A method according to claim 1, wherein the electronic message is received using a mobile electronic communication device.

3. A method according to any preceding claim, wherein the electronic message is received using a communications-enabled computer.

4. A method according to claim 1, wherein the electronic message is transmitted from a secure computer network and received by a mobile electronic communications device.

5. A method according to any preceding claim, wherein the electronic message is transmitted in the form of a text message under the short messaging service (SMS) protocol.

6. A method according to any one of claims 1 to 4, wherein the electronic message is transmitted in the form of an email.
7. A method according to any preceding claim, wherein a different pseudorandom security string is used for each verification transaction.

8. A system for a receiver of an electronic message to authenticate an identity of a sender of the electronic message, the system comprising a receiving device and a transmitting device that are operable to communicate electronically with each other; wherein the receiving device includes a memory containing at least one receiver-side non-repeating pseudorandom string of characters and the transmitting device includes a memory containing at least one transmitter-side non-repeating pseudorandom string of characters identical to the receiver-side pseudorandom string and a user-specific PIN in the form of a first sequence of digits; wherein the transmitter device further includes a processor to generate a one-time security code in the form of a sequence or pattern of characters by applying the user-specific PIN so as to sequentially select numerical positions in the sender-side pseudorandom string on the basis of the numbers in the user-specific PIN, taken in positional order, and returning the characters thereby selected from the sender-side pseudorandom string in sequence so as to form the one-time security code; wherein the transmitter is configured to transmit an electronic message including the one-time security code to the receiver; and wherein the receiver is configured, upon receipt of the message, to correlate the characters in the one-time security code with characters in the receiver-side pseudorandom string by considering the characters of the one-time security code in sequence and identifying a numerical position of each character of the one-time security code in the receiver-side pseudorandom array to thereby generate second sequence of digits; and wherein the identity of the sender is authenticated when the second sequence of digits matches the user-specific PIN.

9. A system as claimed in claim 8, wherein the receiving device is a mobile electronic communication device.

10. A system as claimed in claim 8 or 9, wherein the receiving device is a communications-enabled computer.

11. A system as claimed in any one of claims 8 to 10, wherein the receiving device is a mobile phone or smart phone or the like, and the transmitting device is part of a secure computer network at an official institution, the method and system of the present invention being well-suited for to allow individuals to verify that electronic messages purportedly sent to them by official institution, are in fact authentic.
12. A system as claimed in any one of claims 8 to 11, wherein the electronic message is a text message under the short messaging service (SMS) protocol.

13. A system as claimed in any one of claims 8 to 11, wherein the electronic message is an email.

14. A system as claimed in any one of claims 8 to 13, wherein a different pseudorandom security string is used for each verification transaction.

15. A system as claimed in claim 14, wherein the transmitter and the receiver each run identical secure pseudorandom string generating algorithms in synchronism with each other.

16. A system as claimed in claim 14, wherein the transmitter and the receiver each have a memory, wherein the memories each contain identical sets of pseudorandom strings, and wherein the transmitter and receiver are configured to step through the strings in synchrony for sequential verification transactions.

17. A system as claimed in claim 14, wherein the transmitter is configured to generate a new pseudorandom string after each verification transaction, and then to transmit this new pseudorandom string to the receiver in a separate transmission.

18. A system as claimed in claim 14, wherein the transmitter is configured to generate batches of pseudorandom strings and to transmit these periodically to the receiver, without any one-time security codes, so that the receiver has a supply of pseudorandom strings that can be used in a predetermined sequence with matching transmitter-side pseudorandom security strings.

19. A method for a receiver of an electronic message to authenticate an identity of a sender of the electronic message substantially as hereinbefore described.

20. A system for a receiver of an electronic message to authenticate an identity of a sender of the electronic message substantially as hereinbefore described.
Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

<table>
<thead>
<tr>
<th>Category</th>
<th>Relevant to claims</th>
<th>Identity of document and passage or figure of particular relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>1-18</td>
<td>GB 2387702 A (CELECTIVITY) See whole document</td>
</tr>
<tr>
<td>X</td>
<td>1-18</td>
<td>US 2002/0029342 A1 (KEECH) See whole document in particular figure 11</td>
</tr>
<tr>
<td>X</td>
<td>1-18</td>
<td>US 2005/0246764 A1 (DEBRITO) See whole document in particular figure 3</td>
</tr>
<tr>
<td>X</td>
<td>1-18</td>
<td>EP 1271887 A1 (NOKIA) See whole document in particular figure 3</td>
</tr>
<tr>
<td>A</td>
<td>-</td>
<td>GB 2434472 A (CRAYMER ET AL)</td>
</tr>
</tbody>
</table>

Categories:

| X | Document indicating lack of novelty or inventive step |
| Y & | Document indicating lack of inventive step if combined with one or more other documents of same category. |
| A | Member of the same patent family |
| P | Document published on or after the declared priority date but before the filing date of this invention. |
| E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC:

G06F: G06Q: H04L

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC

International Classification:

<table>
<thead>
<tr>
<th>Subclass</th>
<th>Subgroup</th>
<th>Valid From</th>
</tr>
</thead>
<tbody>
<tr>
<td>H04L</td>
<td>0009/32</td>
<td>01/01/2006</td>
</tr>
<tr>
<td>G06Q</td>
<td>0020/40</td>
<td>01/01/2012</td>
</tr>
</tbody>
</table>