REMOTE USER AUTHENTICATION AND APPARATUS VERIFICATION

FIELD OF THE INVENTION

The present invention relates to user authentication and apparatus verification. More particularly, remote user authentication and verification of an apparatus capable of displaying or generating a one-time passcode (OTP), which may be the card number associated with a pre-paid scratch card or a one-time password generated by an OTP security token, are achieved by means of an unencrypted security code transformed from a user security code and the OTP.

BACKGROUND OF THE INVENTION

Without the use of application-level cryptographic protection, conventional pre-paid cards are not directly usable for mobile payment, reload and remittance applications as user-submitted card numbers in clear text may be intercepted along the paths of communication between the user mobile devices and the remote server application hosted by a service provider. This is particularly vulnerable when mobile originated payment messages are routed through communications gateways, such as short message services (SMS) gateways, over which the operator providing such payment and remittance services has little control.

The present invention ensures secure payment transactions by accomplishing user authentication and card verification without resorting to additional data encryption other than that provided by the native cellular systems. The requirements for such additional encryption capabilities are not easily achieved in mass-market cellular telephony devices as a result of limited device processing power available for cryptographic computations, complex encryption key management and tedious hardware and software installation necessary for enabling user mobile devices to protect data as desired. The problems have hindered the commercialization of general mobile payment applications.

The present invention transforms the unique card number of a pre-paid card with a user security code using a transformation function. The user security code and transformation function are secrets shared between the user and the service provider. The transformed security code, which can easily be worked out or looked up by the user, is sent to the payment operator or service provider via a mobile device. No application-level encryp-

tion is required to protect the payment text message. Each transformed security code is embedded with sufficient information for the service provider to perform card verification as well as user authentication.

The present invention is effective against a variety of security attacks including brute force, dictionary, replay, phishing and Man-in-the-Middle attacks.

In the above-described mobile payment application, the pre-paid cards are the apparatus to be verified and the card number printed and protected on each of the pre-paid cards is the unique one-time passcode (OTP) known to the service provider. In addition, the present invention can be used to boost the security level of a general OTP verification process employed in a two- or multi-factor authentication system, commonly used to authenticate a user by verifying the user password, login code, and other identifications including session- or time-based OTP generated by a hardware token, mobile application or transmitted from the service provider to the user mobile device via text messaging.

For conventional multi-factor authentication using one-time passcodes, the submitted OTP helps prevent replay attacks. Nonetheless, the use of conventional OTP has little effect on the prevention of phishing and Man-in-the-Middle attacks in which the OTP together with the user credentials are intercepted, such as using a forged website, by an imposter for illegitimate use. Thereby, the present invention can be used to strengthen general OTP applications.

SUMMARY OF THE INVENTION

A method of remote user authentication and apparatus verification is provided. In the method, a user has knowledge of a user security code (C_{user}'), an apparatus one-time passcode (C_{OTP}') associated with an apparatus and a transformation function (f_t') associated with the apparatus one-time passcode (OTP) or the user, and a service provider system has system database for storing records of a plurality of valid user identifiers, a plurality of valid user security codes (C_{user}) one of which may match the user security code C_{user}', a plurality of valid appliance one-time passcodes (C_{OTP}) one of which may match the apparatus one-time passcode C_{OTP}', and a plurality of valid transformation functions (f_t) each of which is associated with at least one of the valid appliance one-time passcodes C_{OTP} or at least one of the user identifiers, and the method begins with the user deriving a transformed security code C_T' using the user security code C_{user}', apparatus one-time passcode C_{OTP}' and the transformation function f_t', followed by the user submitting the

transformed security code C_T' to the service provider system, followed by the service provider system retrieving and identifying a valid user security code C_{user} associated with the user, followed by the service provider system examining the valid user security code C_{user} retrieved, the submitted transformed security code C_T', the valid apparatus one-time passcodes C_{OTP} and valid transformation functions f_t in a verification process wherein the service provider system determines whether the submitted transformed security code C_T' can be mapped to any one of the valid apparatus one-time passcodes C_{OTP}, and the user being a legitimate user and the apparatus being a legitimate apparatus if the verification process yields a positive outcome in which the submitted transformed security code C_T' can be mapped to one valid apparatus one-time passcode C_{OTP}.

Each of the apparatus one-time passcodes C_{OTP}', user security code C_{user}', transformed security code C_T', valid apparatus one-time passcodes C_{OTP} and valid user security codes C_{user} is a data string comprising a plurality of characters which belong to a character set S comprising one or a plurality of character types including alphabets, numbers, ideograms and logograms of any language, and the members of the character set S being assigned with position values derived from a predetermined transformation, sequence or lookup table that uniquely maps each member of S to a value indicating, directly or indirectly, the positions of the members in S.

The transformation function f_t' is capable of uniquely mapping an apparatus one-time passcode C_{OTP}' and a user security code C_{user}' to a transformed security code C_T', and each of the valid transformation functions f_t is capable of uniquely mapping a valid apparatus one-time passcode C_{OTP} and a valid user security code C_{user} to a possible transformed security code (p_C_T) used for comparison against the transformed security code C_T' submitted by the user in the verification process.

The transformation function f_t' comprises a mapping function f_m' that uses the user security code C_{user}' to convert K out of the total of I characters of the apparatus one-time passcode C_{OTP}' to K transformed characters which are combined with the remaining (K – I) un-transformed characters of the apparatus one-time passcode C_{OTP}' to form the transformed security code C_T', and each of the valid transformation functions f_t comprises a mapping function f_m which uses the valid user security code C_{user} to convert K out of the total of I characters of the corresponding valid apparatus one-time passcode C_{OTP} to K transformed characters which are combined with the remaining (K – I) un-transformed characters of the valid apparatus one-time passcode C_{OTP} to form the possible trans-

formed security code p_C_T, where I is the number of characters in each of the apparatus one-time passcode C_{OTP}', valid apparatus one-time passcode C_{OTP}, transformed security code C_T' and possible transformed security codes p_C_T, and K is the number of transformed characters and the number of characters in the user security code C_{user}' and valid user security code C_{user}, and I is greater than or equal to K.

The positions of the un-transformed characters in the transformed security code C_T' and possible transformed security code p_C_T may be identical to their respective positions in the apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} respectively. The positions of the transformed characters in the transformed security code C_T' and possible transformed security code p_C_T may be identical to their respective positions in the apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} respectively.

Each of the valid transformation functions may be an inverse of the f_t and denoted as f_t^{-1}, and f_t^{-1} comprises an inverse mapping function f_m^{-1} which is an inverse of the f_m, and f_m^{-1} uses the valid user security code C_{user} to recover the K original characters of the apparatus one-time passcode C_{OTP}' from the K transformed characters out of the total of I characters of the received transformed security code C_T' and the K original characters are combined with the remaining (K – I) un-transformed characters of the received transformed security code C_T' to recover the apparatus one-time passcode C_{OTP}'.

The mapping function f_m' may derive each of the transformed characters in the transformed security code C_T' by replacing the characters to be transformed in the apparatus one-time passcode C_{OTP}' by the corresponding characters of the user security code C_{user}', and the mapping function f_m may derive each of the transformed characters in the possible transformed security code p_C_T by replacing the characters to be transformed in the valid apparatus one-time passcode C_{OTP} by the corresponding characters of the valid user security code C_{user}.

The mapping function f_m' may derive each of the transformed characters in the transformed security code C_T' using a mapping process in which the position of each of the transformed characters in the character set S is the position value of the character to be transformed offset by a value associated with the position value of the corresponding character of the user security code C_{user}' in the same character set S, and the mapping function f_m may derive each of the transformed characters in the possible transformed security code p_C_T using a mapping process in which the position of each of the transformed

characters in the character set S is the position value of the character to be transformed offset by a value associated with the position value of the corresponding character of the valid user security code C_{user} in the same character set S. The mapping process may be a count up process in which the position of each of the transformed characters in the character set S is the position value of the character to be transformed incremented by the position value of the corresponding character of the user security code C_{user}' or valid user security code C_{user} in the character set S. The mapping process may also be a count down process in which the position of each of the transformed characters in the character set S is the position value of the character to be transformed subtracted by the position value of the corresponding character of the user security code C_{user}' or valid security code C_{user} in the character set S. The position value of each of the transformed characters may be subtracted by the total number of characters in the character set S if the position value is greater than the total number of characters in the character set S, and the position value of each of the transformed characters may be incremented by the total number of characters in the character set S if the position value is less than the total number of characters in the character set S.

The mapping function f_m' may be a random function mapping each of the apparatus one-time passcode C_{OTP}' characters to be transformed and the corresponding character of the user security code C_{user}' to the corresponding transformed character, and the mapping function f_m may also be a random function mapping each of the valid apparatus one-time passcode C_{OTP} characters to be transformed and the corresponding character of the valid user security code C_{user} to the corresponding transformed character. The possible inputs and outputs of the random mapping function f_m' may be printed or displayed on the apparatus in the form of a lookup table tabulating transformed characters as a function of each of the possible characters in the user security code C_{user}' and, if applicable, of each of the possible characters to be transformed.

The positions of the characters to be transformed in the apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} may be selected by the user and the service provider system may not have prior knowledge of the positions of the characters to be transformed. The verification process begins with the service provider system retrieving sequentially or systematically the valid apparatus one-time passcodes C_{OTP} and their respective valid transformation functions f_t stored in the system database, the process further evaluates all the possible transformed security codes p_C_T for each of the valid ap-

paratus one-time passcodes C_{OTP} retrieved using the valid user security code C_{user} identified, the corresponding valid transformation function f_t retrieved and all possible combinations of the positions of the characters to be transformed, the process further determines whether any of the possible transformed security codes p_C_T evaluated being identical to the transformed security code C_T' submitted by the user, and if one of the possible transformed security codes p_C_T evaluated being identical to the transformed security code C_T', then the verification process terminating with a positive outcome, otherwise the service provider system will retrieve the next valid apparatus one-time passcode C_{OTP} and the corresponding valid transformation function f_t, and repeat the above-the steps until the verification process has produced a positive outcome or all the valid apparatus one-time passcodes C_{OTP} stored in the system database have been retrieved for examination in the verification process. The verification process may begin with the service provider system retrieving sequentially or systematically the valid apparatus one-time passcodes C_{OTP} and their respective valid transformation functions f_t^{-1} stored in the system database, followed by evaluating all the possible apparatus one-time passcodes (p_C_{OTP}) for the received transformed security code C_T' using the valid user security code C_{user} identified, the corresponding valid transformation function f_t^{-1} retrieved and all possible combinations of the positions of the characters to be transformed, followed by determining whether any of the possible apparatus one-time passcodes p_C_{OTP} evaluated being identical to the valid apparatus one-time passcode C_{OTP} retrieved, and if one of the possible apparatus one-time passcodes p_C_{OTP} evaluated being identical to the valid apparatus one-time passcode C_{OTP} retrieved, then the verification process terminating with a positive outcome, otherwise the service provider system will retrieve the next valid apparatus one-time passcode C_{OTP} and the corresponding valid transformation function f_t^{-1}, and repeat the above-the steps until the verification process has produced a positive outcome or all the valid apparatus one-time passcodes C_{OTP} stored in the system database have been retrieved for examination in the verification process.

The service provider system may have prior knowledge of the positions of the characters to be transformed in the apparatus one-time passcode C_{OTP}' and the service provider system may have the positions of the characters to be transformed stored in the system database. The positions of the characters to be transformed may be displayed, labelled, highlighted or marked on the apparatus for the user to derive the transformed security code C_T'. The verification process may begin with the service provider system retriev-

ing sequentially or systematically the valid apparatus one-time passcodes C_{OTP}, their respective valid transformation functions f_t and positions of transformed characters stored in the system database, followed by evaluating the possible transformed security code p_C_T for each of the valid apparatus one-time passcodes C_{OTP} retrieved using the valid user security code C_{user} identified and the corresponding valid transformation function f_t retrieved, followed by determining whether the possible transformed security code p_C_T evaluated being identical to the transformed security code C_T' submitted by the user, and if the possible transformed security code p_C_T evaluated being identical to the transformed security code C_T', then the verification process terminating with a positive outcome, otherwise the service provider system will retrieve the next valid apparatus one-time passcode C_{OTP}, the corresponding valid transformation function f_t and positions of transformed characters, and repeat the above-the steps until the verification process has produced a positive outcome or all the valid apparatus one-time passcodes C_{OTP} stored in the system database have been retrieved for examination in the verification process. The verification process may also begin with the service provider system retrieving sequentially or systematically the valid apparatus one-time passcodes C_{OTP}, their respective valid transformation functions f_t^{-1} and positions of transformed characters stored in the system database, followed by evaluating the possible apparatus one-time passcode p_C_{OTP} for the submitted transformed security code C_T' using the valid user security code C_{user} identified and the corresponding valid transformation function f_t^{-1} retrieved for each of the valid apparatus one-time passcodes C_{OTP}, followed by determining whether the possible apparatus one-time passcode p_C_{OTP} value evaluated being identical to the valid apparatus one-time passcode C_{OTP} retrieved, and if the possible apparatus one-time passcode p_C_{OTP} evaluated being identical to the valid apparatus one-time passcode C_{OTP} retrieved, then the verification process terminating with a positive outcome, otherwise the service provider system will retrieve the next valid apparatus one-time passcode C_{OTP}, the corresponding valid transformation function f_t^{-1} and positions of transformed characters, and repeat the above-the steps until the verification process has produced a positive outcome or all the valid apparatus one-time passcodes C_{OTP} stored in the system database have been retrieved for examination in the verification process.

The apparatus may be a pre-paid stored value card carrying a unique apparatus OTP which is a card security code printed under an opaque security seal that can be scratched off by the user to reveal the apparatus OTP, and the security seal is designed

for one-time use to prevent the user to re-seal after the seal has been broken, opened, lifted or removed. The positions of the characters to be transformed may be highlighted or marked on the pre-paid stored value card and printed under the opaque security seal. The transformation function f_t' may be printed on the pre-paid stored value card under the opaque security seal. The mapping function f_m' may be printed on the pre-paid stored value card under the opaque security seal. The valid apparatus one-time passcodes C_{OTP} stored in the system database being the card OTPs or card numbers of all the issued pre-paid stored value cards.

The apparatus may be an OTP generator with the generated OTP values C_{OTP}' known to the service provider system. The positions of the characters to be transformed may be displayed on the OTP generator. The transformation function f_t' may be displayed on the OTP generator. The mapping function f_m' may be displayed on the OTP generator. The OTP generator can be of any type including hardware OTP token, software OTP generation applications executed on mobile devices and computing devices, and OTP sent to the user's mobile device.

The user security code C_{user}' is a secret shared between the user and the service provider system and the user security code C_{user}' may be set or chosen by the user or assigned by the service provider system. The user identifier may be a user identification number, a calling party identification number, or the user telephone number. The transformed security code C_T' may be submitted to the service provider system via a telecommunications link including cellular link, mobile link and the Internet via emails, online web access over the Internet, wireless application protocol (WAP) and general packet radio service (GPRS), as well as short message services (SMS) and equivalent messaging applications.

A system for remote user authentication and apparatus verification is provided. The system comprises an apparatus possessed by a user capable of displaying or generating an apparatus one-time passcode (C_{OTP}'), a user security code (C_{user}') being a shared secret between the user and a service provider system, a transformation function (f_t') associated with the apparatus one-time passcode (OTP) or the user, the service provider system has system database for storing records of a plurality of valid user identifiers, a plurality of valid user security codes (C_{user}) one of which may match the user security code C_{user}', a plurality of valid appliance one-time passcodes (C_{OTP}) one of which may match the apparatus one-time passcode C_{OTP}', and a plurality of valid transformation functions (f_t) each of

which is associated with at least one of the valid appliance one-time passcodes C_{OTP} or at least one of the user identifiers, and in the system, the user derives a transformed security code C_T' using the user security code C_{user}', apparatus one-time passcode C_{OTP}' and the transformation function f_t' associated with the apparatus or the user, the user further submits the transformed security code C_T' to the service provider system, the service provider system retrieves a valid user security code C_{user} associated with the user, the service provider system examines the valid user security code C_{user} identified, the submitted transformed security code C_T', the valid apparatus one-time passcodes C_{OTP} and valid transformation functions f_t in a verification process wherein the service provider system determines whether the submitted transformed security code C_T' can be mapped to any one of the valid apparatus one-time passcodes C_{OTP}, and the user being a legitimate user and the apparatus being a legitimate apparatus if the verification process yields a positive outcome in which the submitted transformed security code C_T' can be mapped to one valid apparatus one-time passcode C_{OTP}.

BRIEF DESCRIPTION

Embodiments according to the present invention will now be described with reference to the following figures, in which like reference numerals denote like elements.

FIG. 1 illustrates a mobile payment system configured to implement the user authentication and apparatus verification processes of the present invention.

FIG. 2 illustrates the general data formats of the apparatus OTP / card security code, user security code and transformed security code of FIG. 1.

FIG. 3 illustrates an embodiment of the transformation function of FIG. 1 & FIG. 2.

FIG. 4 illustrates the pre-paid card capable of concealing additional confidential information including the mapping function of FIG. 3.

FIG. 5 illustrates an embodiment of the inverse transformation function stored in the service provider system of FIG. 1.

FIG. 6 illustrates a first embodiment of the verification process flow implemented by the mobile payment system of FIG. 1 using the inverse transformation function of FIG. 5.

FIG. 7 illustrates a second embodiment of the verification process flow implemented by the mobile payment system of FIG. 1.

FIG. 8 illustrates a mobile or online application configured to implement the general multi-factor user authentication and OTP verification processes of the present invention.

DETAILED DESCRIPTION

FIG. 1 illustrates a mobile payment system configured to implement the user authentication and apparatus verification processes of the present invention.

Pre-paid stored value cards 110 each of which carries a unique apparatus one-time passcode C_{OTP}' 120 in the form of a card security code 120 printed under an opaque security seal 115 are provided. A user acquires one of the pre-paid cards 110 and scratches off the opaque security seal 115 to reveal the card security code C_{OTP}' 120. The user further evaluates a transformed security code C_T' 140 by transforming the revealed card security code C_{OTP}' 120 with a user security code C_{user}' 130 and a transformation function f_t' 150.

Primed symbols denote variables, parameters and constants associated with codes and functions known to the user, whereas symbols without any prime denote variables, parameters and constants associated with codes and functions stored in the database of the service provider system 165.

The user security code C_{user}' 130 is a secret shared between the user and the service provider system 165. The transformation function f_t' 150 is a simple operation which the user can easily perform. The user further submits a payment request comprising the transformed security code C_T' 140 to the service provider system 165 via his or her mobile device (158) over a communication link 160 established between the user mobile device and the service provider system 165. The transformation function f_t' 150 is known to both the user and the service provider. f_t' 150 may be associated with one or a plurality of pre-paid cards 110. f_t' 150 may also be associated with one or a plurality of users.

Upon receiving the transformed security code C_T' 140, the service provider system 165 identifies the user, through verification against the valid user ID records 171 stored in a user records database 170, and retrieves the corresponding valid user security code C_{user} 172 from the database 170. The service provider system 165 further scans through each of the valid card security codes C_{OTP} 176, which are the card numbers of all the issued pre-paid cards 110 registered in a card records database 175, and retrieves the corresponding valid transformation functions f_t 177 from the card database 175. The retrieved valid user security codes C_{user} 172, valid card security codes C_{OTP} 176 and the corre-

sponding valid transformation functions f_t 177 are used by the service provider system 165 to derive a plurality of possible transformed security codes p_C_T for comparison against the received transformed security code C_T' 140 in the verification process 180. User authentication and card verification are successful if one of the possible transformed security codes p_C_T is identical to the received transformed security code C_T' 140 submitted by the user.

If the inverse of the valid transformation functions f_t^{-1} 178 are available, the service provider system 165 may alternatively use the received transformed security code C_T' 140, the valid user security codes C_{user} 172 retrieved from the user database 170 and said inverse transformation functions f_t^{-1} 178 retrieved from the card database 175 to compute a plurality of possible card security codes p_C_{OTP} for comparison against each of the valid card security codes C_{OTP} 176 retrieved from the card database 175. User authentication and card verification are successful if one of the possible card security codes p_C_{OTP} derived is identical to one of the valid card security codes C_{OTP} 176.

Successful user authentication and card verification prove that the user knows his secret user security code C_{user}' 130, the one-time card security code C_{OTP}' 120 and the corresponding transformation function f_t' 150. The service provider system 165 advances to execute the applicable payment processes in step 190 in accordance with the received payment request 158 if the user authentication and card verification are positive. Otherwise, the service provider system 165 rejects the payment request 158, and may update the applicable system records in the database 170 & 175 and inform the user accordingly.

The service provider system 165 may identify the user from the identity he claims in the payment request that comprises the submitted transformed security code C_T' 140 (158). The user identification may also be accomplished by matching the calling party identification number or caller ID, which is typically the telephone number of the user mobile device, against all the user identification numbers 171 registered in the user database 170 of the service provider system 165.

The apparatus OTP or C_{OTP}' 120 is printed on the pre-paid card 110 which may be made from materials that provide sufficient mechanical support. The security seal 115 and the part of the pre-paid card where the card security code C_{OTP}' 120 and any accompanying confidential information, such as the transformation function f_t' 150, must not allow sufficient penetration of light, infra-red, x-ray or other electromagnetic sources such that the

printed C_{OTP}' 120 and any accompanying confidential information can be read before the security seal 115 has been removed.

The security seal 115 allows the user to scratch off without considerable effort. The security seal 115 is designed for one-time use and it does not allow the user to re-seal the protected data after the seal 115 has been broken, opened, lifted or removed. Thereby, the card security code C_{OTP}' 120 is a predetermined one-time passcode valid for one transaction. The pre-paid card 110 may carry printed graphics, pre-paid currency and value, expiry date, usage terms and conditions, instructions and any other information related to the use of the card, card issuer and service provider.

Without loss of generality, the pre-paid card 110 may be integrated with a magnetic tape for storing parameters necessary for on-site card verification when a magnetic reader is available. The pre-paid card 110 may also be integrated with a smart processor chip for storing parameters and executing applications necessary for on-site card verification when a smart chip reader is available.

The user may submit the transformed security code C_T' 140 to the service provider via an electronic, online or telecommunication link 160 between the user and the service provider system 165. The link 160 may include but are not limited to any of the fixed-line, wireless, mobile and cellular links supporting analogue or digital data transmission, which may further comprise any of the circuit-switched, packet-switched communication and point-to-point protocols. Thus, C_T' 140 may be submitted via emails, online web access over the Internet, wireless application protocol (WAP) and general packet radio service (GPRS), as well as short message services (SMS) and equivalent messaging applications.

FIG. 2 illustrates the general data formats of the apparatus OTP / card security code, user security code and transformed security code of FIG. 1.

The apparatus OTP or card security code C_{OTP}' 120 is a data string printed on a pre-paid card 110 and concealed by the security seal 115. The user may scratch the security seal off to review the printed data string. As shown in Equation 1 and depicted in FIG. 2, the C_{OTP}' 120 is a data string comprising a total of I symbols or characters s_{ci}'.

$$C_{OTP}' = s_{c1}'\, s_{c2}'\, s_{c3}' \ldots s_{ci}' \ldots s_{cI}' \quad \text{, where} \quad 1 \le i \le I \qquad \text{(Eq 1)}$$

Each C_{OTP}' 120 is typically randomly generated. The C_{OTP}' 120 may be randomly selected from a vast data set having all the possible combinations of characters s_{ci}'. The probability of having two identical C_{OTP}' 120 is sufficiently low, and this probability is de-

pendent upon the number of characters used in C_{OTP}' 120 and the total number of possible values of s_{ci}'.

The user security code C_{user}' 130 is known only to the user and the service provider. C_{user}' 130 is used to transform the C_{OTP}' 120 to form the transformed security code C_T' 140. As shown in Equations 2 & 3 and depicted in FIG. 2, C_{user}' 130 is a data string comprising a total of K characters s_{uk}' whereas C_T' 140 is a data string comprising a total of N characters s_{tn}'.

$$C_{user}' = s_{u1}' s_{u2}' s_{u3}' s_{u4}' \ldots s_{uk}' \ldots s_{uK}' \quad \text{,where} \quad 1 \leq k \leq K \qquad \text{(Eq 2)}$$

$$C_T' = s_{t1}' s_{t2}' s_{t3}' s_{t4}' \ldots s_{tn}' \ldots s_{tN}' \quad \text{,where} \quad 1 \leq n \leq N \qquad \text{(Eq 3)}$$

The user security code C_{user}' 130 is a shared secret between the user and the service provider. The user security code C_{user}' 130 is assigned by the service provider prior to any authentication and verification request. The user security code C_{user}' 130 may also be chosen by the user and approved by the service provider. As a good security practice, C_{user}' 130 may be changed on a regular basis.

The user submits the transformed secured code C_T' 140 to the service provider for user authentication and card verification, and the service provider proceeds to process payment if said user authentication and card verification results are positive. In general, C_T' 140 is derived through the application of a predetermined transformation function f_t' 150 to all or typically parts of the one-time apparatus or card security code C_{OTP}'120. Given a card security code C_{OTP}' 120 and a user security code C_{user}' 130, the transformation function f_t' 150 yields a unique transformed security code C_T' 140, as expressed mathematically in Equation 4.

$$C_T' = f_t' (C_{OTP}', C_{user}') \qquad \text{(Eq 4)}$$

The transformation function f_t' 150 is known to both the user and the service provider. f_t' 150 may be associated with one or a plurality of pre-paid cards 110. f_t' 150 may also be associated with one or a plurality of users. Deriving the transformed security code C_T' 140 requires the knowledge of both of the card and user security codes C_{OTP}' 120 & C_{user}' 130.

Since the user security code C_{user}' 130 and the transformation function f_t' 150 are known only to the user who submits the payment request 158, whereas the card security code C_{OTP}' 120 is a short-lived one-time passcode (OTP), thus the present invention is effectively an OTP-based two-factor authentication and verification scheme. Furthermore, the present invention is effectively an OTP based three-factor authentication and verifica-

tion when the user submits said transformed security code C_T' 140 to the service provider via his or her mobile telephony device whose identification comprising the telephone number has been registered with the service provider prior to any authentication attempt.

The characters s_{ci}', s_{uk}' and s_{tn}' that make up C_{OTP}' 120, C_{user}' 130 and C_T' 140 respectively are elements belonging to a character set S comprising alphabets, numbers, symbols, ideograms and logograms of any language, as shown in Equation 5.

$$s_{ci}', s_{uk}', s_{tn}' \in S \quad \text{(Eq 5)}$$

The members of the character set S are assigned with position values. Thereby all the members of S may be arranged in ascending or descending orders of their position values. The position values may be derived from a predetermined transformation, sequence or lookup table that uniquely maps each member of S to a value indicating, directly or indirectly, the positions of the members in S. The sequence may be based upon the ordering of English alphabets, numerals, and any of the character encoding schemes such as ASCII (American Standard Code for Information Exchange), GB18030 and other Unicode schemes.

FIG. 3 illustrates an embodiment of the transformation function of FIG. 1 & FIG. 2. The transformation function f_t' 150 uses the user security code C_{user}' 130 to map K characters 305, out of the total I characters, of the card security code C_{OTP}' 120 to a new set of transformed characters denoted by $\underline{s}_{tn}$' 320. The transformation function f_t' 150 is mathematically expressed in Equation 6.

$$f_t': \begin{cases} \underline{s}_{tn}'|_{n=i=io} = f_m'(s_{ci}'|_{i=io}, s_{uk}') & \text{for a total of K characters at predetermined or user selected positions } i = i_o, \text{ whereas } f_m \text{ is a mapping function } \& \ K \leq I \\ s_{tn}'|_{n=i} = s_{ci}' & \text{elsewhere (i.e. } i \neq i_o) \end{cases} \quad \text{(Eq 6)}$$

The positions of the K transformed characters $\underline{s}_{tn}$' 320 are either predetermined for each card or randomly selected by the user. Any predetermined positions of the transformed characters $\underline{s}_{tn}$' 320 are registered (179) in the server card database 175 for each issued pre-paid card 110. The predetermined positions may be marked or highlighted clearly on the pre-paid card 110 and are concealed by the security seal 115.

As an example, the card security code C_{OTP}' 120 has twelve randomly generated characters (I = 12), and the user security code C_{user}' 130 is made up of two user-selected

characters (K = 2) that are approved by the service provider. Furthermore, the predetermined positions of the characters 305 to which the transformation function f_t' 150 is applied are $n = i_o = 2$ & 5, then Equations 1, 2 & 3 become

$C_{OTP}' = s_{c1}' s_{c2}' s_{c3}' s_{c4}' s_{c5}' s_{c6}' s_{c7}' s_{c8}' s_{c9}' s_{c10}' s_{c11}' s_{c12}'$

$C_{user}' = s_{u1}' s_{u2}'$

$C_T' = s_{t1}' \underline{s}_{t2}' s_{t3}' s_{t4}' \underline{s}_{t5}' s_{t6}' s_{t7}' s_{t8}' s_{t9}' s_{t10}' s_{t11}' s_{t12}'$

$= s_{c1}' \underline{s}_{c2}' s_{c3}' s_{c4}' \underline{s}_{c5}' s_{c6}' s_{c7}' s_{c8}' s_{c9}' s_{c10}' s_{c11}' s_{c12}'$

In a second example, the card security code C_{OTP}' 120 has 15 randomly generated alphanumeric characters, and the user security code C_{user}' 130 is made up of 3 numerals assigned by the service provider. Furthermore, the user has randomly chosen to transform the characters at the 3rd, 6th & 10th positions, then I = 16, K = 3 and $n = i_o = 3$, 6 & 10 and Equations 1, 2 & 3 become

$C_{OTP}' = A\ 1\ 5\ F\ 3\ A\ 0\ B\ 3\ X\ D\ Z\ 0\ G\ G$

$C_{user}' = 2\ 8\ 5$

$C_T' = s_{c1}' s_{c2}' \underline{s}_{c3}' s_{c4}' s_{c5}' \underline{s}_{c6}' s_{c7}' s_{c8}' s_{c9}' \underline{s}_{c10}' s_{c11}' s_{c12}' s_{c13}' s_{c14}' s_{c15}'$

$= A\ 1\ \underline{7}\ F\ 3\ \underline{I}\ 0\ B\ 3\ \underline{C}\ D\ Z\ 0\ G\ G$

Where

$f_m'(5, 2) = 7$, $f_m'(A, 8) = I$ and $f_m'(X, 5) = C$

The mapping function f_m' 310 is known to both the user and the service provider. The mapping function f_m' 310 uses the user security code C_{user}' 130 to transform each of the chosen characters 305 in the printed card security code C_{OTP}' 120 to a transformed character $\underline{s}_{tn}'$ 320 as in Equation 7. There is no restriction to the mapping function used.

$$\underline{s}_{tn}' = f_m'(s_{ci}', s_{uk}') \quad \text{(Eq 7)}$$

In a first embodiment of the mapping function 310, f_m' 310 performs simple transformation which can easily be handled by the user manually, without resorting to any computational tool. A simple yet effective implementation is expressed in Equations 8a & 8b.

$$f_m': \begin{cases} pos(\underline{s}_{tn}') = pos(s_{ci}') + pos(s_{uk}') & \text{(Eq 8a)} \\ \quad \text{where } pos(s') = \text{the position value of s' in the character set S} \\ pos(\underline{s}_{tn}') = pos(\underline{s}_{tn}') - \text{MaxPos} & \text{(Eq 8b)} \\ \quad \text{if } pos(\underline{s}_{tn}') \text{ is larger than the maximum position value of S denoted by MaxPos.} \end{cases}$$

As an example, if S = {1, 2, 3, 4, 5, 6, 7, 8 , 9, 0, A, B, … , X, Y, Z}, then *pos(5)* = 5 & *pos(2)* = 2, and *pos(5)* + *pos(2)* = 7 which corresponds to the numeral "7" in S. Therefore, f_m' (5, 2) = 7. In practice, the user can mentally work out "7" as the transformed character 320 by performing a count-up of the card C_{OTP}' character "5" using an increment of 2. In addition, *pos(X)* = 34 and *pos(5)* = 5. Thus *pos(X)* + *pos(5)* = 39 which is larger than the maximum position value of MaxPos = 36. Therefore, *pos(X)* + *pos(5)* = 39 – 36 = 3 which corresponds to the numeral "3" in S. In practice, the user can mentally work out "3" as the transformed character 320 by performing a count-up of the card character "X" using an increment of 5, with the next character being looped back to "1" after counting up to "Z".

Other functions based upon counting-down and skip-counting may be used as the mapping function f_m' 310.

Evaluation of the transformed characters $\underline{s}_{tn}'$ 320 by the user can further be simplified if the character set S contains only numerals S = {1, 2, 3, 4, 5, 6, 7, 8, 9, 0}. In this case, the card security number C_{OTP}' 120 and user security number C_{user}' 130 are made up of numerals which greatly simplify the counting task required by the mapping function f_m' 310.

The mapping function f_m' 310 may be a direct substitution with the chosen card characters in C_{OTP}' 120 replaced by the user characters in C_{user}' 130 as shown in Equation 9. This mapping function is very simple to use but it is more susceptible to replay attacks.

$$f_m' : \quad \underline{s}_{tn}' = s_{uk}' \qquad \text{(Eq 9)}$$

The mapping function f_m' 310 or reminder information related to the mapping function may be printed on the pre-paid card 110 and concealed by the security seal 115.

FIG. 4 illustrates the pre-paid card capable of concealing additional confidential information including the mapping function of FIG. 3.

In a second embodiment of the mapping function 310, f_m' 310 performs more complex transformation which may take the user considerable effort to work out the transformed characters $\underline{s}_{tn}'$ 320 mentally. In this embodiment, the information necessary for the user to evaluate the transformed characters 320 may be printed on the pre-paid card 110, and concealed by the same opaque security seal 115 used to protect the card security number C_{OTP}' 120. The information may be a mapping function 310 in the form of a lookup table which allows the user to find the transformed characters $\underline{s}_{tn}$ 320 readily.

If the positions of the transformed characters $\underline{s}_{tn}$' 320 are predetermined, then the predetermined positions 410 may be marked or highlighted clearly on the pre-paid card 110 and are concealed by the security seal 115.

One of the advantages of providing the table on the pre-paid card allows the use of different mapping functions f_m' 310 for different groups of pre-paid cards 110. It also allows the use of a unique mapping function f_m' 310 for each individual pre-paid card 110. This results in higher level of security as it is harder for an imposter to execute an illegitimate attack without prior knowledge of the mapping function f_m' 310 applicable to a particular pre-paid card 110.

In order to assign a unique mapping function f_m' 310 applicable to one and only one pre-paid card 110, each transformed character $\underline{s}_{tn}$' 320 may be randomly mapped to each combination of the character pairs s_{uk}' and s_{ci}', which is expressed in Equation 10.

$$f_m' : \quad \underline{s}_{tn}' = \text{Random}(s_{ci}', s_{uk}') \qquad \text{(Eq 10)}$$

Alternatively speaking, each mapping function f_m' 310 is a random function known to the service provider and the user in the form of a lookup table printed on the pre-paid card 110 and concealed with the security seal 115.

The mapping function f_m' 310 in Equation 10 may be simplified to Equation 11 such that the characters to be transformed s_{ci}' in the one-time passcode C_{OTP}' 120 are dummy and they are not used by the random mapping function. As such, the number of elements in each said lookup table is minimized. Thus, the card area required to print the table is minimized.

$$f_m' : \quad \underline{s}_{tn}' = \text{Random}\,(s_{uk}') \qquad \text{(Eq 11)}$$

FIG. 5 illustrates an embodiment of the inverse transformation function stored in the service provider system of FIG. 1.

The user and card data including the transformation functions (C_{OTP} 176, C_{user} 172 & f_t 177) that are stored in the service provider system 165 have the same structures and formats as those (C_{OTP}' 120, C_{user}' 130 & f_t' 150) possessed by the user. Thus, valid card security codes C_{OTP} 176 and the valid user security codes C_{user} 172 stored in the system user database 170 and card database 175 can be represented by Equations 1 and 2 with the prime notations removed; the possible transformed security codes p_C_T derived by the service provider system 165 are represented by Equations 3 and 4 with the prime notations removed, as represented mathematically in Equations 12 – 16 below:

$$C_{OTP} = s_{c1}\, s_{c2}\, s_{c3} \ldots s_{ci} \ldots s_{cl} \quad \text{, where} \quad 1 \le i \le l \qquad \text{(Eq 12)}$$

$C_{user} = s_{u1}\, s_{u2}\, s_{u3}\, s_{u4} \ldots s_{uk} \ldots s_{uK}$, where $1 \leq k \leq K$ (Eq 13)

$p_C_T = s_{t1}\, s_{t2}\, s_{t3}\, s_{t4} \ldots s_{tn} \ldots s_{tN}$, where $1 \leq n \leq N$ (Eq 14)

$p_C_T = f_t(C_{OTP}, C_{user})$ (Eq 15)

with

$s_{ci}, s_{uk}, s_{tn} \in S$ (Eq 16)

The valid transformation functions f_t 177 may be associated with one or a plurality of the valid appliance one-time passcodes C_{OTP} 176. f_t 177 may also be associated with one or a plurality of the valid user identifiers 171. If a pre-paid card security code C_{OTP}' 120 is identical to a valid card security code C_{OTP} 176, then their respective transformation functions f_t' 150 and f_t 177 are always identical to each other, or $f_t' = f_t$. f_t 177 uses a valid user security code C_{user} 172 to map K characters, out of the total I characters, of a valid card security code C_{OTP} 176 to a new set of transformed characters denoted by $\underline{s}_{tn}$. The transformation function f_t 177 is mathematically expressed in Equation 17 below.

$$f_t: \begin{cases} \underline{s}_{tn}|_{n=i=io} = f_m(s_{ci}|_{i=io}, s_{uk}) & \text{for a total of K characters at predetermined or user selected positions } i = i_o, \text{ whereas } f_m \text{ is a valid mapping function and } K \leq I \\ s_{tn}|_{n=i} = s_{ci} & \text{elsewhere (i.e. } i \neq i_o) \end{cases} \quad \text{(Eq 17)}$$

The positions of the K transformed characters $\underline{s}_{tn}$ are either predetermined for each card or randomly selected by the user. Any predetermined positions of the transformed characters $\underline{s}_{tn}$ are registered in the server card database 175 for each issued pre-paid card 110.

There is no restriction to the valid mapping function f_m used, f_m may be identical to those expressed in Equations 8 – 10 for f_m' 310.

The inverse transformation function f_t^{-1} 178 is the inverse of the transformation function f_t 177. f_t^{-1} 178 is used to evaluate the possible card security codes p_C_{OTP} 550, given the valid user security code C_{user} 172 retrieved from system user database 170 and the received transformed security code C_T' 140. The possible card security codes p_C_{OTP} 550 are used in the verification process 180 for determining whether any one of p_C_{OTP} 550 is identical to any one of the valid card security codes C_{OTP} 176 stored in the system card database 175.

f_t^{-1} 178 therefore can be expressed as

$s_{ci} = f_t^{-1}(\underline{s}_{tn}', s_{uk})$ (Eq 18)

where

$$f_t^{-1} = (f_t')^{-1} \quad \text{(Eq 19)}$$

Each f_t^{-1} 178 performs inverse transformation on the transformed characters $\underline{s}_{tn}'|_{n=i=io}$ 320 to derive $s_{ci}|_{i=io}$ 505 in the possible card security code p_C_{OTP} 550. f_t^{-1} 178 is expressed in Equation 20.

$$f_t^{-1}: \begin{cases} s_{ci}|_{i=io} = f_m^{-1}(\underline{s}_{tn}'|_{n=i=io}, s_{uk}) & \text{(Eq 20)} \\ \quad \text{for a total of K characters at positions } i = i_o, \text{ and } K \leq I \\ s_{ci} = s_{tn}|_{n=i} \quad \text{elsewhere (i.e. } i \neq i_o) \end{cases}$$

where f_m^{-1} 510 is the inverse of the mapping function f_m' 310 as shown in Equation 21.

$$f_m^{-1} = (f_m')^{-1} \quad \text{(Eq 21)}$$

FIG. 6 illustrates a first embodiment of the verification process flow implemented by the mobile payment system of FIG. 1 using the inverse transformation function of FIG. 5. Each transformed security code C_T' 140 submitted by the user is embedded with sufficient information for the service provider to perform card verification as well as user authentication. The first verification process flow 600 is a first embodiment of the verification process 180 (Fig. 1).

The first verification process flow 600 begins with step 610 when the service provider system 165 has received the user payment request sent (158) from the user mobile device. In step 610, the process 600 retrieves the user identifier from the request message. Alternatively, the service provider system 165 may retrieve the user identifier from the caller line identification number or the caller telephone number which is used directly as the user identifier. The caller telephone number may serve as a pointer to records that comprise the user identifier. The service provider system 165 compares the retrieved user identifier against the valid user ID 171 stored in system user database 170. If the retrieved user identifier is invalid, then the process 600 terminates (not shown), otherwise the retrieved user identifier enables the service provider system 165 to look up the valid user security code C_{user} 172, which is associated with the user, stored in the system user database 175 in step 620. The process 600 proceeds to steps 630 and 640 in which the valid card security code C_{OTP} 176 and the inverse transformation function f_t^{-1} 178 of the first issued card entry stored in the card records database 175 are respectively retrieved. The first verification process 600 determines in step 650 whether the positions of the transformed characters $\underline{s}_{tn}$ (Equation 17) are predetermined, which may be indicated by any

data entry in the corresponding card records database 175 registering said transformed characters positions 179 associated with each issued pre-paid card.

If the exact positions (n = i_o) of the transformed characters $\underline{s}_{tn}$ are not known, the process 600 evaluates in step 680 all the possible card security codes p_C_{OTP} 550. Each of the possible card security codes p_C_{OTP} 550 can be evaluated by assuming the position values n = i_o of the transformed characters $\underline{s}_{tn}$. All the possible card security codes p_C_{OTP} 550 can be evaluated by using all possible combinations of position values n = i_o in the inverse transformation function f_t^{-1} 178 retrieved in step 640. As an example, the valid user security code C_{user} 172 is made up of two characters (K = 2) and each valid card security code C_{OTP} 176 has a length of twelve characters (I = 12), then the inverse transformation function f_t^{-1} 178 yields $_{12}C_2$ = 66 possible card security codes p_C_{OTP} 550 each of which corresponds to one combination of the position values i_o.

Next, the first verification process 600 advances to step 690 to compare each of the possible card security codes p_C_{OTP} 550 derived against the valid card security code C_{OTP} 176 retrieved in step 630. If there is a positive match found in step 690, the first verification process 600 ends in step 695 with the matched possible card security code p_C_{OTP} 550 being the card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user. If no positive match is found in step 690, the first verification process 600 loops back to step 630 to retrieve the next valid card security code C_{OTP} 176 stored in system card database 175, followed by retrieving in step 640 the corresponding inverse transformation function f_t^{-1} 178 stored in the database 175.

If it is found in step 650 that the exact positions (n = i_o) of the transformed characters $\underline{s}_{tn}$ are predetermined, the first verification process 600 retrieves in step 660 the stored positions of the transformed characters 179 from the system card database 175, which are used in the inverse transformation function f_t^{-1} 178 to compute a possible card security code p_C_{OTP} 550. The first verification process 600 then advances to step 670 to compare the computed card security code p_C_{OTP} 550 against the valid card security code C_{OTP} 176 retrieved in step 630. If there is a positive match found in step 670, the first verification process 600 ends in step 695 with the matched possible or valid card security code C_{OTP} 176 being the card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user. If no positive match is found in step 690, the first verification process 600 loops back to step 630 to retrieve the next valid card security code C_{OTP} 176, followed by retrieving in

step 640 the corresponding inverse transformation function f_t^{-1} 178 stored in the card records database 175.

The steps 630 through 690 are repeated until either a positive match is found or when all the valid card security codes C_{OTP} 176 stored have been examined.

The service provider system 165 advances to execute the applicable payment processes in step 190 (FIG. 1) in accordance with the received payment request 158 if the user authentication and card verification are positive. Otherwise, the service provider system 165 rejects the payment request 158, and may update the applicable system records and inform the user accordingly.

The first verification process 600 can be simplified when a common inverse transformation function f_t^{-1} 178 is applicable to *all or a subset* of the issued pre-paid cards 110, as it is not necessary to retrieve each valid card security code C_{OTP} 176 one by one as is done is step 630. For the case of *unknown positions* of the transformed characters $\underline{s}_{tn}$' 320 in the received transformed security code C_T' 140, all possible card security codes p_C_{OTP} 550 are first evaluated using the single inverse transformation function f_t^{-1} 178, and in the same manner as the execution in step 680. By now, the service provider system 165 has known a group of possible card security codes p_C_{OTP} 550 and a batch of valid card security codes C_{OTP} 176. To evaluate the card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user, the provider system 170 would only need to find a positive match between the group of possible card security codes p_C_{OTP} 550 and the batch of valid card security codes C_{OTP} 176. The first verification process 600 ends regardless of whether a positive match has been identified. For the case of the transformed characters $\underline{s}_{tn}$ having *predetermined positions*, the service provider system 165 retrieves the stored positions of the transformed characters 179, which are used in the inverse transformation function f_t^{-1} 178 to compute one possible card security code p_C_{OTP} 550. The verification process 600 then advances to compare the computed card security code p_C_{OTP} 550 against all the valid card security codes C_{OTP} 176. To evaluate the card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user, the service provider system 165 would only need to find a positive match between the computed card security code p_C_{OTP} 550 and the batch of valid card security codes C_{OTP} 176. The verification process 600 ends regardless of whether a positive match has been identified.

After successful user authentication and card verification, the records of the used pre-paid card 110 are removed from the database 175 or a status record is updated to reflect that the prepaid card 110 has been activated and it has no more stored value.

When matching against all the possible card security codes p_C_{OTP} 550 in step 690, the valid card security codes C_{OTP} 176 may be searched with the aid of a quick-search index derived and registered in the system card records database 175 when the card security number records of any newly issued pre-paid cards 110 are initially created in the database 175. There is no limitation to the algorithm used for the quick-search index provided that the use of the index helps narrowing down the number of possible pre-paid cards that the user may have purchased and activated. Shorter search time can be accomplished with the service provider system 165 scanning all card records and identifying cards having quick-search indices that are sufficiently close to the index derived for the received transformed security code C_T' 140. Each index does not necessarily to be uniquely mapped to one and only one valid card security code C_{OTP} 176. In an embodiment, the quick-search index for a particular pre-paid card is the sum of the position values of all the characters in the corresponding one-time passcode. This algorithm involves simple arithmetic and is of high computational efficiency.

FIG. 7 illustrates a second embodiment of the verification process flow implemented by the mobile payment system of FIG. 1.

In this embodiment, the valid transformation functions f_t 177 together with the valid user security codes C_{user} 172 and the corresponding valid card security codes C_{OTP} 176 retrieved from the system database 170 & 175 are used by the service provider system 165 to derive a plurality of possible transformed security codes p_C_T (Equations 14 & 15) for comparison against the received transformed security code C_T' 140.

The second verification process 700 begins with step 710 when the service provider system 165 has received the user payment request sent (158) from the user mobile device. In step 710, the second verification process 700 retrieves the user identifier from the request message. Alternatively, the service provider system 165 may retrieve the user identifier from the caller line identification number or the caller telephone number which is used directly as the user identifier. The caller telephone number may serve as a pointer to records that comprise the user identifier. The service provider system 165 compares the retrieved user identifier against the valid user ID 171 stored in system user database 170. If the retrieved user identifier is invalid, then the process 700 terminates (not shown), oth-

erwise the retrieved user identifier enables the service provider system 165 to look up the valid user security code C_{user} 172, which is associated with the user, stored in the system database 175 in step 720. The process 700 proceeds to steps 730 and 740 in which the valid card security code C_{OTP} 176 and the transformation function f_t 177 of the first issued card entry stored in the card records database 175 are respectively retrieved. The second verification process 700 determines in step 750 whether the positions of the transformed characters $\underline{s}_{tn}$ (Equation 17) are predetermined, which may be indicated by some appropriate data entry in the corresponding card records database 175 registering said transformed characters positions associated with each card.

If the exact positions (n = i_o) of the transformed characters $\underline{s}_{tn}$ are not known, the process 700 evaluates in step 780 all the possible transformed security codes p_C_T. Each of the possible transformed security codes p_C_T can be evaluated by assuming the position values i_o of the transformed characters $\underline{s}_{tn}$. All the possible transformed security codes p_C_T can be evaluated by using all possible combinations of position values i_o in the valid transformation function f_t 177 retrieved in step 740. Next, the second verification process 700 advances to step 790 to compare each of the possible transformed security codes p_C_T derived against the received transformed security code C_T' 140. If there is a positive match found in step 790, the second verification process 700 ends in step 795 with the matched possible transformed security code p_C_T being the transformed security code C_T' 140 the user sent in. The card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user can be regenerated using the matched p_C_T, the valid transformation function f_t 177 retrieved in step 740 and the valid user security code C_{user} 172 retrieved in step 720. If no positive match is found in step 790, the second verification process 700 loops back to step 730 to retrieve the next valid card security code C_{OTP} 176, followed by retrieving in step 740 the corresponding valid transformation function f_t 177 stored in the card records database 175.

If it is found in step 750 that the exact positions (n = i_o) of the transformed characters $\underline{s}_{tn}$ are predetermined, the process 700 retrieves in step 760 the stored positions of the transformed characters 179, which are used in the valid transformation function f_t 177 to compute a possible transformed security code p_C_T. The second verification process 700 then advances to step 770 to compare the computed transformed security code p_C_T against the received transformation security code C_T' 140. If there is a positive match found in step 770, the process 700 ends in step 795 with the matched computed trans-

formed security code p_C_T being the transformed security code C_T' 140 the user sent in. The card security code C_{OTP}' 120 of the pre-paid card 110 possessed by the user can be regenerated using the matched transformed security code p_C_T, the valid transformation function f_t 177 retrieved in step 740 and the valid user security code C_{user} 172 retrieved in step 720. If no positive match is found in step 790, the second verification process 700 loops back to step 730 to retrieve the next valid card security code C_{OTP} 176, followed by retrieving in step 740 the corresponding transformation function f_t 177 stored in the card records database 175.

The steps 730 through 790 are repeated until either a positive match is found or when all the valid card security codes C_{OTP} 176 stored have been examined.

The service provider system 165 advances to execute the applicable payment processes in step 190 (FIG. 1) in accordance with the received payment request 158 if the user authentication and card verification are positive. Otherwise, the service provider system 165 rejects the payment request 158, and may update the applicable system records and inform the user accordingly.

After successful user authentication and card verification, the records of the used pre-paid card 110 are removed from the database 175 or a status record is updated to reflect that the prepaid card 110 has been activated and it has no more stored value.

FIG. 8 illustrates a mobile or online application configured to implement the general multi-factor user authentication and OTP verification processes of the present invention.

It has generally been recognized that in general multi-factor authentication using one-time passcodes (OTP), the submitted OTP helps prevent replay attacks but it is not effective in preventing phishing and Man-in-the-Middle attacks in which the OTP together with the user credentials are intercepted, such as using a forged website, by an imposter for illegitimate use. It should be apparent to those skilled in the art that the present invention can readily be applied to any form of one-time passcodes generated by hardware or software applications in tokens, mobile telephony devices, computers and other devices, with the card security codes used for pre-paid card replaced by said generated OTP.

The user obtains an appliance one-time passcode C_{OTP}' 820 from an OTP generator, which may be a hardware token, software application or sent via text messaging from a service provider such as a bank, online or mobile payment operator. The user further evaluates a transformed security code C_T' 140 (Equation 3) by transforming the C_{OTP}' 820 (Equation 1) with a user security code C_{user}' 130 (Equation 2) and a transformation function

f_t' 150 (Equation 6). The user security code C_{user}' 130 is a secret shared between the user and a service provider system 865. The transformation function f_t' 150 is a simple operation which the user can easily perform. The user further submits a service request comprising the transformed security code C_T' 140 to the service provider system 865 via his or her mobile or online application (858) over a communication link 860 established between the user mobile or online application and the remote service provider system 865.

Upon receiving the transformed security code C_T' 140, the service provider system 865 identifies the user , through verification against the valid user ID records 171 stored in a user records database 170, and retrieves the corresponding valid user security code C_{user} 172 from a user records database 170. The service provider system 865 further derives the valid C_{OTP} (830) using a predetermined OTP algorithm and predetermined parameters shared between the user and the service provider. The service provider system 865 retrieves the corresponding transformation function f_t 177 (Equation 17) or inverse transformation function f_t^{-1} 178 (Equation 20) and the positions of the transformed characters $\underline{s}_{tn}$, if available, from the transformation records database 875. The transformation function f_t' 150 is known to the user before the service request, or it may be generated and displayed by the user OTP generator. The valid transformation functions f_t 177 or f_t^{-1} 178 is also known to the service provider system 865 before the service request, or the same function may be generated by the service provider system 865 in synchronization with the transformation function f_t' 150 generated by the above-said user OTP generator. This may be accomplished through the use of a predetermined transformation function algorithm and associated parameters shared between the user and the service provider.

The retrieved valid user security code C_{user} 172, derived C_{OTP} 830, and the valid transformation function f_t 177 are used by the service provider system 865 to derive the corresponding possible transformed security codes p_C_T for comparison against the received transformed security code C_T' 140 in the verification process in step 180 (FIG. 7). User authentication and card verification (180) are successful if one of the derived transformed security codes and the received transformed security code are identical.

If the inverse of the valid transformation function f_t^{-1} 178 is available, the service provider system 865 may alternatively use the received transformed security code C_T' 140, the valid user security code C_{user} 172 retrieved from the user database 170 and said inverse transformation function f_t^{-1} 178 retrieved from the database 875 to compute the corresponding possible appliance security codes p_C_{OTP} 550 for comparison against each of

the valid C_{OTP} derived in process 830. User authentication and card verification (180 & FIG. 6) are successful if one of the possible OTPs and the OTP derived in process 830 are identical. Successful user authentication and card verification (180) prove that the user knows his secret user security code C_{user}' 130, the appliance OTP C_{OTP}' 820 and the corresponding transformation function f_t' 150.

The service provider system 865 advances to execute the applicable payment processes in step 890 in accordance with the received service request 858 if the user authentication and card verification are positive. Otherwise, the service provider system 865 rejects the service request 858, and may update the applicable system records and inform the user accordingly.

The service provider system 865 may identify the user from the identity he claims in the service request that comprises the submitted transformed security code C_T' 140 in the process 858. The user identification may also be accomplished by matching the calling party identification number or caller ID, which is typically the telephone number of the user mobile device, against all the user identification numbers registered in the database 170 of the service provider system 865.

The user may submit the transformed security code C_T' 140 to the service provider via an electronic, online or telecommunication link 860 between the user and the service provider. The link 860 may include but are not limited to any of the fixed-line, wireless, mobile and cellular links supporting analogue or digital data transmission, which may further comprise any of the circuit-switched, packet-switched communication and point-to-point protocols. Thus, C_T' 140 may be submitted via emails, online web access over the Internet, wireless application protocol (WAP) and general packet radio service (GPRS), as well as short message services (SMS) and equivalent messaging applications.

Although the above description contains much specificity, these should not be construed as limiting the scope of the embodiments but merely providing illustration of the foreseeable embodiments. Especially the above stated advantages of the embodiments should not be construed as limiting the scope of the embodiments but merely to explain possible achievements if the described embodiments are put into practise. Thus, the scope of the embodiments should be determined by the claims and their equivalents, rather than by the examples given.

CLAIMS

1. A method of remote user authentication and apparatus verification, wherein

a user has knowledge of a user security code (C_{user}'), an apparatus one-time passcode (C_{OTP}') associated with an apparatus and a transformation function (f_t') associated with said apparatus one-time passcode or said user,

a service provider system has system database for storing records of a plurality of valid user identifiers, a plurality of valid user security codes (C_{user}) one of which may match said user security code C_{user}', a plurality of valid appliance one-time passcodes (C_{OTP}) one of which may match said apparatus one-time passcode C_{OTP}', and a plurality of valid transformation functions (f_t) each of which is associated with at least one of said valid appliance one-time passcodes C_{OTP} or at least one of said user identifiers, and

the method comprising the steps of

said user deriving a transformed security code C_T' using said user security code C_{user}', apparatus one-time passcode C_{OTP}' and said transformation function f_t',

said user submitting said transformed security code C_T' to said service provider system,

said service provider system retrieving and identifying a valid user security code C_{user} associated with said user,

said service provider system examining said valid user security code C_{user} retrieved, said submitted transformed security code C_T', said valid apparatus one-time passcodes C_{OTP} and valid transformation functions f_t in a verification process wherein said service provider system determines whether said submitted transformed security code C_T' can be mapped to any one of said valid apparatus one-time passcodes C_{OTP}, and

said user being a legitimate user and said apparatus being a legitimate apparatus if said verification process yields a positive outcome in which said submitted transformed security code C_T' can be mapped to one valid apparatus one-time passcode C_{OTP}.

2. The method of claim 1, wherein

each of said apparatus one-time passcodes C_{OTP}', user security code C_{user}', transformed security code C_T', valid apparatus one-time passcodes C_{OTP} and valid user security codes C_{user} being a data string comprising a plurality of characters which belong to a character set S comprising one or a plurality of character types including alphabets, numbers,

ideograms and logograms of any language, and the members of the character set S being assigned with position values derived from a predetermined transformation, sequence or lookup table that uniquely maps each member of S to a value indicating, directly or indirectly, the positions of the members in S.

3. The method of claim 1, wherein

said transformation function f_t' being capable of uniquely mapping an apparatus one-time passcode C_{OTP}' and a user security code C_{user}' to a transformed security code C_T', and each of said valid transformation functions f_t being capable of uniquely mapping a valid apparatus one-time passcode C_{OTP} and a valid user security code C_{user} to a possible transformed security code (p_C_T) used for comparison against said transformed security code C_T' submitted by said user in said verification process.

4. The method of claims 1 or 3, wherein

said transformation function f_t' comprising a mapping function f_m' that uses said user security code C_{user}' to convert K out of the total of I characters of said apparatus one-time passcode C_{OTP}' to K transformed characters which are combined with the remaining (K – I) un-transformed characters of said apparatus one-time passcode C_{OTP}' to form said transformed security code C_T', and

each of said valid transformation functions f_t comprising a mapping function f_m which uses said valid user security code C_{user} to convert K out of the total of I characters of said corresponding valid apparatus one-time passcode C_{OTP} to K transformed characters which are combined with the remaining (K – I) un-transformed characters of said valid apparatus one-time passcode C_{OTP} to form said possible transformed security code p_C_T,

where I being the number of characters in each of said apparatus one-time passcode C_{OTP}', valid apparatus one-time passcode C_{OTP}, transformed security code C_T' and possible transformed security codes p_C_T, and K being the number of transformed characters and the number of characters in said user security code C_{user}' and valid user security code C_{user}, and I being greater than or equal to K.

5. The method of claim 4, wherein

the positions of said un-transformed characters in the transformed security code C_T' and possible transformed security code p_C_T are identical to their respective positions in

said apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} respectively.

6. The method of claims 4 or 5, wherein

the positions of said transformed characters in said transformed security code C_T' and possible transformed security code p_C_T are identical to their respective positions in said apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} respectively.

7. The method of any of claims 1, 3 to 6, wherein

each of said valid transformation functions being an inverse of said f_t and denoted as f_t^{-1}, and f_t^{-1} comprising an inverse mapping function f_m^{-1} which is an inverse of said f_m, and f_m^{-1} uses said valid user security code C_{user} to recover the K original characters of said apparatus one-time passcode C_{OTP}' from the K transformed characters out of the total of I characters of said received transformed security code C_T' and said K original characters are combined with the remaining (K – I) un-transformed characters of said received transformed security code C_T' to recover said apparatus one-time passcode C_{OTP}'.

8. The method of any of claims 4 to 6, wherein

said mapping function f_m' deriving each of said transformed characters in said transformed security code C_T' by replacing the characters to be transformed in said apparatus one-time passcode C_{OTP}' by the corresponding characters of said user security code C_{user}', and

said mapping function f_m deriving each of said transformed characters in said possible transformed security code p_C_T by replacing the characters to be transformed in said valid apparatus one-time passcode C_{OTP} by the corresponding characters of said valid user security code C_{user}.

9. The method of any of claims 2, 4 to 6, wherein

said mapping function f_m' deriving each of said transformed characters in said transformed security code C_T' using a mapping process in which the position of each of said transformed characters in said character set S is the position value of the character to be

transformed offset by a value associated with the position value of the corresponding character of said user security code C_{user}' in said same character set S, and

said mapping function f_m deriving each of said transformed characters in said possible transformed security code p_C_T using a mapping process in which the position of each of said transformed characters in said character set S is the position value of the character to be transformed offset by a value associated with the position value of the corresponding character of said valid user security code C_{user} in said same character set S.

10. The method of claim 9, wherein

said mapping process being a count up process in which the position of each of said transformed characters in said character set S is the position value of the character to be transformed incremented by the position value of the corresponding character of said user security code C_{user}' or valid user security code C_{user} in said character set S.

11. The method of claim 9, wherein

said mapping process being a count down process in which the position of each of said transformed characters in said character set S is the position value of the character to be transformed subtracted by the position value of the corresponding character of said user security code C_{user}' or valid security code C_{user} in said character set S.

12. The method of any of claims 9 to 11, wherein

the position value of each of said transformed characters being subtracted by the total number of characters in said character set S if said position value is greater than the total number of characters in said character set S, and

the position value of each of said transformed characters being incremented by the total number of characters in said character set S if said position value is less than the total number of characters in said character set S.

13. The method of any of claims 4 to 6, wherein

said mapping function f_m' being a random function mapping each of said apparatus one-time passcode C_{OTP}' characters to be transformed and the corresponding character of said user security code C_{user}' to the corresponding transformed character, and

said mapping function f_m being a random function mapping each of said valid apparatus one-time passcode C_{OTP} characters to be transformed and the corresponding character of said valid user security code C_{user} to the corresponding transformed character.

14. The method of claim 13, wherein

the possible inputs and outputs of said random mapping function f_m' being printed or displayed on said apparatus in the form of a lookup table tabulating transformed characters as a function of each of the possible characters in said user security code C_{user}' and, if applicable, of each of the possible characters to be transformed.

15. The method of any of claims 1, 3 to 6, wherein

said positions of the characters to be transformed in said apparatus one-time passcode C_{OTP}' and valid apparatus one-time passcode C_{OTP} being selected by said user, and said service provider system having no prior knowledge of said positions of the characters to be transformed.

16. The method of any of claims 1, 3 to 6 and 15 wherein

said verification process comprising the steps of

said service provider system retrieving sequentially or systematically said valid apparatus one-time passcodes C_{OTP} and their respective valid transformation functions f_t stored in said system database,

evaluating all the possible transformed security codes p_C_T for each of said valid apparatus one-time passcodes C_{OTP} retrieved using said valid user security code C_{user} identified, the corresponding valid transformation function f_t retrieved and all possible combinations of the positions of said characters to be transformed,

determining whether any of said possible transformed security codes p_C_T evaluated being identical to said transformed security code C_T' submitted by said user, and

if one of said possible transformed security codes p_C_T evaluated being identical to said transformed security code C_T', then said verification process terminating with a positive outcome, otherwise said service provider system will retrieve the next valid apparatus one-time passcode C_{OTP} and the corresponding valid transformation function f_t, and repeat the above-said steps until said verification process has produced a positive outcome or all

said valid apparatus one-time passcodes C_{OTP} stored in said system database have been retrieved for examination in said verification process.

17. The method of claims 1, 7 or 15 wherein

said verification process comprising the steps of

said service provider system retrieving sequentially or systematically said valid apparatus one-time passcodes C_{OTP} and their respective valid transformation functions f_t^{-1} stored in said system database,

evaluating all the possible apparatus one-time passcodes (p_C_{OTP}) for said received transformed security code C_T' using said valid user security code C_{user} identified, the corresponding valid transformation function f_t^{-1} retrieved and all possible combinations of the positions of said characters to be transformed,

determining whether any of said possible apparatus one-time passcodes p_C_{OTP} evaluated being identical to said valid apparatus one-time passcode C_{OTP} retrieved, and

if one of said possible apparatus one-time passcodes p_C_{OTP} evaluated being identical to said valid apparatus one-time passcode C_{OTP} retrieved, then said verification process terminating with a positive outcome, otherwise said service provider system will retrieve the next valid apparatus one-time passcode C_{OTP} and the corresponding valid transformation function f_t^{-1}, and repeat the above-said steps until said verification process has produced a positive outcome or all said valid apparatus one-time passcodes C_{OTP} stored in said system database have been retrieved for examination in said verification process.

18. The method of any of claims 1, 3 to 6, wherein

said service provider system having prior knowledge of said positions of the characters to be transformed in said apparatus one-time passcode C_{OTP}' and said service provider system having said positions of the characters to be transformed stored in said system database.

19. The method of claim 18, wherein

said positions of the characters to be transformed being displayed, labelled, highlighted or marked on said apparatus for said user to derive said transformed security code C_T'.

20. The method of any of claims 1, 3 to 6 and 18 to 19 wherein

said verification process comprising the steps of

said service provider system retrieving sequentially or systematically said valid apparatus one-time passcodes COTP, their respective valid transformation functions ft and positions of transformed characters stored in said system database,

evaluating the possible transformed security code p_C_T for each of said valid apparatus one-time passcodes C_{OTP} retrieved using said valid user security code C_{user} identified and the corresponding valid transformation function f_t retrieved,

determining whether said possible transformed security code p_C_T evaluated being identical to said transformed security code C_T' submitted by said user, and

if said possible transformed security code p_C_T evaluated being identical to said transformed security code C_T', then said verification process terminating with a positive outcome, otherwise said service provider system will retrieve the next valid apparatus one-time passcode C_{OTP}, the corresponding valid transformation function f_t and positions of transformed characters, and repeat the above-said steps until said verification process has produced a positive outcome or all said valid apparatus one-time passcodes C_{OTP} stored in said system database have been retrieved for examination in said verification process.

21. The method of claims 1, 7, 18 or 19, wherein

said verification process comprising the steps of

said service provider system retrieving sequentially or systematically said valid apparatus one-time passcodes C_{OTP}, their respective valid transformation functions f_t^{-1} and positions of transformed characters stored in said system database,

evaluating a possible apparatus one-time passcode p_C_{OTP} for said submitted transformed security code C_T' using said valid user security code C_{user} identified and the corresponding valid transformation function f_t^{-1} retrieved for each of said valid apparatus one-time passcodes C_{OTP},

determining whether said possible apparatus one-time passcode p_C_{OTP} value evaluated being identical to said valid apparatus one-time passcode C_{OTP} retrieved, and

if said possible apparatus one-time passcode p_C_{OTP} evaluated being identical to said valid apparatus one-time passcode C_{OTP} retrieved, then said verification process terminating with a positive outcome, otherwise said service provider system will retrieve the next valid apparatus one-time passcode C_{OTP}, the corresponding valid transformation func-

tion f_t^{-1} and positions of transformed characters, and repeat the above-said steps until said verification process has produced a positive outcome or all said valid apparatus one-time passcodes C_{OTP} stored in said system database have been retrieved for examination in said verification process.

22. The method of any of claims 1 to 21, wherein

said apparatus being a pre-paid stored value card carrying a unique apparatus one-time passcode which is a card security code printed under an opaque security seal that can be scratched off by said user to reveal said apparatus one-time passcode, and said security seal being designed for one-time use to prevent said user to re-seal after the seal has been broken, opened, lifted or removed.

23. The method of claims 19 or 22, wherein

said positions of the characters to be transformed being highlighted or marked on said pre-paid stored value card and printed under said opaque security seal.

24. The method of any of claims 3 to 6, 8 to 14 and 22, wherein

said transformation function f_t' being printed on said pre-paid stored value card under said opaque security seal.

25. The method of any of claims 3 to 6, 8 to 14 and 22, wherein

said mapping function f_m' being printed on said pre-paid stored value card under said opaque security seal.

26. The method of any of claims 1 to 6, 8, 13, 15 to 17 and 20 to 21, wherein

said valid apparatus one-time passcodes C_{OTP} stored in said system database being the card one-time passcodes or card numbers of all the issued pre-paid stored value cards.

27. The method of any of claims 1 to 21, wherein

said apparatus being a one-time passcode (OTP) generator with the generated OTP values C_{OTP}' known to said service provider system.

28. The method of any of claims 8 to 11, 13 to 17, 19, 23 and 27, wherein

said positions of the characters to be transformed being displayed on said OTP generator.

29. The method of any of claims 3 to 6, 8 to 14 and 27, wherein

said transformation function f_t' being displayed on said OTP generator.

30. The method of any of claims 3 to 6, 8 to 14 and 27, wherein

said mapping function f_m' being displayed on said OTP generator.

31. The method of any of claims 27 to 30, wherein

said OTP generator can be of any type including hardware OTP token, software OTP generation applications executed on mobile devices and computing devices, and OTP sent to said user's mobile device.

32. The method of any of claims 1 to 31, wherein

said user security code C_{user}' being a secret shared between said user and said service provider system and said user security code C_{user}' being set or chosen by said user or assigned by said service provider system.

33. The method of claim 1, wherein

said user identifier being a user identification number, a calling party identification number, or the user telephone number.

34. The method of claim 1, wherein

said transformed security code C_T' being submitted to said service provider system via a telecommunications link including cellular link, mobile link and the Internet via emails, online web access over the Internet, wireless application protocol (WAP) and general packet radio service (GPRS), as well as short message services (SMS) and equivalent messaging applications.

35. A system for remote user authentication and apparatus verification comprising

an apparatus possessed by a user capable of displaying or generating an apparatus one-time passcode (C_{OTP}'), a user security code (C_{user}') being a shared secret between said user and a service provider system, a transformation function (f_t') associated with said apparatus one-time passcode or said user,

said service provider system having system database for storing records of a plurality of valid user identifiers, a plurality of valid user security codes (C_{user}) one of which may match said user security code C_{user}', a plurality of valid appliance one-time passcodes (C_{OTP}) one of which may match said apparatus one-time passcode C_{OTP}', and a plurality of valid transformation functions (f_t) each of which is associated with at least one of said valid appliance one-time passcodes C_{OTP} or at least one of said user identifiers, wherein

said user deriving a transformed security code C_T' using said user security code C_{user}', apparatus one-time passcode C_{OTP}' and said transformation function f_t' associated with said apparatus or said user, said user further submitting said transformed security code C_T' to said service provider system, said service provider system retrieving a valid user security code C_{user} associated with said user, said service provider system examining said valid user security code C_{user} identified, said submitted transformed security code C_T', said valid apparatus one-time passcodes C_{OTP} and valid transformation functions f_t in a verification process wherein said service provider system determines whether said submitted transformed security code C_T' can be mapped to any one of said valid apparatus one-time passcodes C_{OTP}, and said user being a legitimate user and said apparatus being a legitimate apparatus if said verification process yields a positive outcome in which said submitted transformed security code C_T' can be mapped to one valid apparatus one-time passcode C_{OTP}.