



\*G00002\*

## SECURITY SYSTEMS FOR INTERNET TRANSACTIONS AND METHOD OF USE

This application is a continuation in part of, and claims benefit of the filing date of, and hereby incorporates fully by reference, the pending parent application entitled *Security Systems for Internet Transactions and Method of Use* initially filed as Application No. 200204065-7 filed 12 April 2002.

### DESCRIPTION OF USE



\*159159\*

This invention relates generally to the field of security applications for both financial and information transfer in network applications, in particular internet & intranet applications. The security arrangements can be used between a plurality of types of buyers and one seller, a plurality of types of sellers and one buyer, and a combination of these.

### BACKGROUND OF THE INVENTION

Computer systems are found today in virtually every walk of life for storing, maintaining, and transferring various types of data. The Internet has enabled computers to transcend the constraints of their individual performance capabilities to access a global network of information sources, resources and potential customers.

The opportunity for Internet commerce (e-commerce) has given rise to great opportunities and potential risks for the users. The Internet Protocol (IP) underpinning Internet (as well as the majority of corporate networks) has numerous strengths. Due largely to its flexibly routed packets, in which data is broken up into manageable pieces for transmission over networks, it is powerful, highly efficient, and cost-effective and can be used by any significant operating system.

However, despite these strengths, the current IP was conceived for a completely different operational environment to that of the current internet. Consequently, the Internet is inherently vulnerable to malicious, systematic or inadvertent data insecurity. Due to its method of

routing packets, IP-based networks are vulnerable to spoofing, sniffing, session hijacking, and 'man-in-the-middle' attacks which were not in existence when IP was first introduced.

The integrity of large portions of this internet-transmitted data, especially that portion relating to financial transactions, is vital to the health and survival of many commercial enterprises.

5 Individual consumers also have an increasing stake in data security as open and unsecured data communications channels for sales transactions, such as credit card transactions over the Internet, gain popularity.

Protecting data stored in computer memory, tape, and disk is often important. However, just as important, if not more so, is the ability to transfer financial transactions or other  
10 communications from a sender to an intended receiver without intermediate parties being able to interpret the transferred message. Furthermore, as important transactions are increasingly handled electronically, authentication of the originator of a message must be ensured. For example, for electronic banking, there needs to be a way to authenticate that an electronic document, such as a bank draft, has actually been "signed" by the indicated  
15 signatory.

These factors play a key role in the effectiveness (both actual and perceived) of E-commerce, whether business to business (B2B) or business to end user. The B2B commerce interactions can occur at any point in a given supply chain of services or commodities or a multiplicity of such supply chains.

20 There are two principal difficulties with e-commerce with respect to billing transactions;

- firstly, potential incompatibility between of a plurality of different types of programs and different operating system bases used by businesses wishing to have a high degree of mutual communication regarding billing; and
- secondly, the above-mentioned design characteristics inherent in the Internet protocol  
25 (IP), also leads to almost total lack of security regarding the information conveyed.

Initial attempts for providing security over the internet included application-level protocols and software. Examples of these included SSL (Secure Socket Layer) for securing web traffic, SSH (Secure Shell) for securing Telnet sessions and file transfers, and PGP (Pretty Good Privacy) for securing email. However, these applications are all limited to specific  
5 programs or protocols. Thus where two businesses operate on different applications, the systems may not be able to communicate effectively.

These and many other means of securely sending information on billing via the internet or electronic funds transfer employ security measures with some form of cryptograph. The strength i.e. a measure of the effort required to defeat the encryption, and the usability of the  
10 security measures employed has been found to vary greatly.

Cryptography typically involves converting data from an understandable form into an encrypted form that cannot be understood by persons other than the intended recipient, and transmitting the data to the recipient who deciphers the data. It is useful in many applications, including confidential business communications, military intelligence as well as Internet  
15 commerce and electronic financial services. In each of these applications, it is essential that communications be secure against eavesdropping and unauthorised access.

Encryption of data is usually accomplished by applying an algorithm to that data, and decryption is accomplished by applying the inverse of that algorithm. In many cases, the encryption step involves a "pass phrase" or key, which is combined with the data according to  
20 the algorithm to create the encrypted message, so that it is necessary for the recipient to know both the key and the inverse algorithm in order to decrypt the message.

Cryptography typically serves two purposes. One of these is to ensure that only the intended recipient receives a secret message. This is accomplished by ensuring that only the intended recipient has the key and inverse algorithm necessary to decrypt the message. The other  
25 purpose is "message authentication", which provides assurance to the recipient that the message really did come from the sender. This is accomplished by ensuring that only the

sender has the key and algorithm necessary to encrypt messages which make sense when decrypted by the key and inverse algorithm.

One common form of cryptography is public key cryptography, as described in U.S. Pat. Nos. 4,218,582 and 4,200,770 by Martin E Hellman, Bailey W Diffie and Ralph C Merkle.

5 This involves finding a pair consisting of an algorithm and an inverse algorithm, for which it is impossible (or "computationally infeasible") to determine the inverse algorithm from the original algorithm. One set of such algorithm/inverse pairs is known as the RSA algorithm and is described in U.S. Pat. No. 4,405,829 by Ronald L Rivest, Adi Shamir and Leonard M Adleman. The person who creates the algorithm/inverse pair distributes the algorithm  
10 publicly but keeps the inverse secret. Anyone can then send a secret message to that person by encrypting the message with the algorithm (or "public key"). Only the person with the inverse algorithm (or "secret key") can decrypt any such message. Conversely, message authentication can be achieved if the person encrypts a message with the secret key. Any other person can use the public key to decrypt the message and confirm that it came from the  
15 secret key holder

However, public key cryptography is susceptible to "spoofing", in which a person pretends to be someone else, and sends out a public key under that other person's name. Moreover, because the algorithm/inverse pairs tend to be complex, this method of cryptography typically requires considerable computing resources and is comparatively slow.

20 Another common type of cryptography is known as DES (Data Encryption Standard). This is a block cipher that has become the US Data Encryption Standard. A block cipher involves partitioning the message into blocks, often with some padding to fill out the final block, and then encrypting and transmitting each block. DES uses a 64-bit block with a 56-bit key. DES is one of many different types of secret key cryptography, which depends upon the  
25 secret key being sent by a secured channel from the transmitter to the receiver so that it is kept secret from the rest of the world.

DES and any other secret key security system rely on the vigilance of the users in ensuring the key remains secret. In practice this is difficult to achieve. Furthermore, if the secret key is stolen, it would not be obvious to a recipient of a fraudulent communication that the sender was not the correct entity.

- 5 There are various different ways to break an encryption code without first having had access to the key and/or algorithm. One of these approaches is known as the "codebook" or "dictionary" attack, and it involves sequentially trying all the possible transformations between original message text and encrypted data.

Therefore, one common means of increasing the strength of a security algorithm is by  
10 increasing its data size. Increasing the length of a key from say 32 bits to 56 bits increase the number of possible key permutations from  $4.3 \times 10^9$  to  $7.2 \times 10^{16}$ . However, the computational power of a system used to try the various permutations affects whether the time involved warrants the potential gain from decrypting the data. Using the above comparison of a 32 bit and a 56 bit key, a sampling rate of one key permutation per micro second ( $\mu\text{Sec}$ ) would give  
15 a total time of 36 minutes and 1142 years respectively. Increasing the sampling rate to  $10^6/\pi$  second reduces the above times to  $\sim 2$  milliseconds and  $\sim 10$  hours respectively. By way of further comparison, a 128 bit key would take  $\sim 5 \times 10^{18}$  yrs to conduct an exhaustive search of all the key permutations at sampling rate of  $10^6/\pi$  second. Conversely, using an excessively large key data length creates processing difficulties for the systems tasked with the legitimate  
20 processing of transactions using the key.

Consequently, there is a need to maintain a sufficiently infeasible search time by virtue of the key data length without resulting in an impractical, or undesirable processing time for the users in a legitimate transaction.

US patent no. 4962530 (Cairns) provides a system for randomly changing positions of  
25 indicia, which are represented by a matrix of keys from the keyboard. As this value randomly changes and is visible only to the sender the code is difficult to replicate without matching of

stored values. However, for large interactive systems where a multiple number of end users or sellers are provided, this system is difficult to use efficiently and is slow to operate.

US patent no. 4799156 (Shavit) discloses a system for interactive online communications and processing of business transactions, which involve different types of independent users and buyers and sellers. The system comprises access means for selective access to a database, which is centrally accessible, and in which one party uses the transaction to specifically select another party. However, the level of security is low and does not allow for easy transfer of payment instructions for accounts.

US patent no. 4396914 (Aston) teaches an electronic security device with a memory and a card reader. What are now known as "smart cards" can be used with this device. However, every end user needs a card reader, if this is to be used in conjunction with e-business.

US patent no. 4271482 (Giraud) provides a data processing system protecting confidentiality of key material. The security is provided by a predetermined permanent code key, which controls access to the computer or data after comparison to and recognition of the input code of the user. However, this system requires that the computer or device used and connected to the internet be used by the same user all the time. It is not possible for different computers or connection devices to be used by a multiplicity of users.

US patent no. 4234932 (Gorgens) teaches a security system for remote cash dispensers. A PIN (personal identification number) generated by a random number signal generator, provides the security for an individual person to a remote terminal. The terminal can dispense cash and provide other banking services. However, such terminals are not connected to the internet; they do not provide the ability to conduct e-business with a multiplicity of retailers, only with one central banking system. It is not a system which could be used by a retail end user wishing to conduct e-business, as well as B2B commercial activity on the internet.

US patent no. 4630201 (White) provides both on- and off-line transaction security systems using a code generated from the transaction and from a random number generator. However, this requires a portable transaction device and specialist cards, which are read by the portable transaction device. Thus the system cannot be used in an electronic B2B arrangement, nor  
5 with an electronic retailer and electronic business with a multiplicity of end users and internet interfaces.

US patent no. 4023013 (Kinker) teaches online verification systems for identification of cards and the like. Once again however, a specialist card and card reader is required. Such readers are not generally available in B2B transactions and most retailers of the internet businesses  
10 do not have such card reader systems.

US patent no. 6097307 (Utz) teaches a transmitting unit for a wireless security system, which incorporates randomised successive verification codes. This has specialist use when powering up an integrated circuit, incorporates a pseudo random number generator to warn against unauthorised entry into an automobile and such systems. The particular sequence of  
15 operations, which the system is designed to alert a user to, is not one that is generated during Internet business transactions.

None of the prior art teaches a system that provides a security system usable for both B2B commercial transactions and e-business to retail commercial transactions. Further, none of the prior art teaches a system that can be used regardless of the different types of accounting  
20 systems of each business or retail buyer in a chain of electronic business.

At the present time, the main methods employed for Internet banking, secure transactions and security systems are:

- ID and password with SSL encryption;
- Smart chips/Smart cards;

- RSA SecurID™;
- USB key;
- Bio-Metric.

However, all the above means suffer from disadvantages including;

- 5       - ID and or passwords may be captured by hackers, forgotten by the user, or copied.
- Smart chips/Smart cards are expensive and require dedicated card readers;
- RSA SecurID™ proprietary system employing two-factor authentication is expensive and involves the need for distribution through participating branches:
- USB keys are inconvenient (as a USB port is always required) and expensive; and
- 10       - Bio-metric devices such as fingerprint sensors or retinal scanners are also expensive and inconvenient.

It is clearly desirable for any security means employed to facilitate secure Internet transactions to be usable through a range of communications mediums and retail/commerce outlets. Conventional business cards have now been superseded in some instances by cards  
 15       incorporating a recordable media such as CD-R, CD-RW data or the like. The business card itself thus doubles as both an introductory card in a conventional role plus as a loyalty card, brochures/catalog folio, video presentation, and/or prepaid card for example.

It would thus be desirable to combine the features of such interactive cards with a security authentication card to facilitate secure Internet transactions.

20       It is thus an object of the present invention to preserve the confidentiality of electronic transactions involving funds transfer in electronic business, without needing to be limited to a specific end user computer, specialist equipment for reading 'smart cards' or inputting

encryption coding.

A further object of the invention is providing means for entering a code for identification or authentication, which means allows a secure comparison procedure to be performed electronically and to permit payment for products/services sold electronically, electronic  
5 transfer of funds, and electronic confirmation of all stages of the transaction.

It is an object of the present invention to address the foregoing problems or at least to provide the public with a useful choice.

#### **BRIEF DESCRIPTION OF THE INVENTION**

According to one aspect, the present invention provides a security key for use in online  
10 transactions over electronic networks between users, said users including: at least one client, and at least one recipient, characterised in that each key, includes code generated independently from said client and recipient, characterised in that said code generation includes a first encoding factor wherein a multi-bit code text is at least partly formed from parameters derived from co-ordinates of a point  $P(i)$  on a multi-dimensional sphere..

15 According to a further aspect, the present invention provides a security system for transactions for use in user authentication and for confirmation of transactions over electronic networks said system including online processing of transactions between users, said users including: at least one client, and at least one recipient, wherein each transaction incorporates use of a unique security key, characterised in that said system incorporates computer  
20 processor and memory means for generating each key, said key comprising: code generated independently from said client and recipient by a code engine, said code including at least two encoding factors, said key being regenerated upon each transaction and supplied to said user for storage in a portable recordable medium.

The use of two authentication or encoding factors adds significantly to the strength of the  
25 key, providing a manifold increase in the effort required to break the key and/or cycle through

all the possible data permutations constituting the key code prior to application of the two factor encoding.

The first authentication/encoding factor provides a process that generates a text which is difficult for a potential hacker to predict, yet is able to be reliably and a repeatably generated  
5 by the correct users, is unique, and one which forms part of a sequence of texts enabling the authorised users of the system to generate subsequent texts allowing the security key code to be updated at every transaction.

According to one aspect of the invention, said key includes a first encoding factor comprising a multi-bit text capable of representation as co-ordinates of a point P(i) on a multi-  
10 dimensional sphere. The concept of using points on the surface of a multi-dimensional sphere provides a mathematically rigorous means of generating a text of any desired length.

Whilst it is straightforward for humans to visualise 2 or 3 dimensional geometric entities such as a circle or sphere, visualising abstract higher dimensional entities is difficult. From a mathematical perspective however, extending the geometrical principles involved to higher  
15 number of dimensions is logically sound and well established. Moreover, it provides a means of generating data text for use in security authentication/encryption techniques.

Using 50 dimensions as an example, the co-ordinates ( $x_1[i]$ ,  $x_2[i]$ ,  $x_3[i]$ ,.....  $x_{50}[i]$ ) of a point on a 50-dimension sphere may be defined according to the following equations;

$$x_1[i]=R*\sin(\text{ang}_1).$$

$$20 \quad x_2[i]=R*\cos(\text{ang}_1)*\sin(\text{ang}_2).$$

$$x_3[i]=R*\cos(\text{ang}_1)*\cos(\text{ang}_2)*\sin(\text{ang}_3).$$

.

.

$$x_{49}[i]=R*\cos(\text{ang}_1)*\cos(\text{ang}_2).....\cos(\text{ang}_{48})*\sin(\text{ang}_{49}).$$

$$25 \quad x_{50}[i]=R*\cos(\text{ang}_1)*\cos(\text{ang}_2).....\cos(\text{ang}_{48})*\cos(\text{ang}_{49}),$$

where R is a constant denoting the radius of the sphere.

This formula is an extension of two-dimensional circle and three-dimensional sphere.

The parameter equation of a circle is

$$y=R*\sin(ang).$$

$$5 \quad x=R*\cos(ang).$$

where the parameter 'ang' denotes an angular value from 0 to 360<sup>0</sup>.

The shape transcribed by the point (x,y) through the full parameter range is a circle.

The parameter equation of a sphere is:

$$z=R*\sin(ang_1).$$

$$10 \quad y=R*\cos(ang_1) * \sin(ang_2).$$

$$x=R*\cos(ang_1)* \cos(ang_2).$$

where its parameters ang<sub>1</sub> and ang<sub>2</sub> vary from -90<sup>0</sup> to 90<sup>0</sup> and from 0<sup>0</sup> to 180<sup>0</sup> respectively.,

The shape transcribed by the point (x,y,z) through the specified parameter range is a sphere.

It can be thus seen that the above 50-dimension sphere is an extension of the parametric

15 equations in two and three-dimensions.

Consequently, for an 'n' dimensional sphere may be represented by the equations said

co-ordinates P(i) = (x<sub>1</sub>[i], x<sub>2</sub>[i], x<sub>3</sub>[i],..... x<sub>n</sub>[i]) are given by

$$x_1[i]=R*\sin(ang_1).$$

$$x_2[i]=R*\cos(ang_1)* \sin(ang_2).$$

$$20 \quad x_3[i]=R*\cos(ang_1)* \cos(ang_2)* \sin(ang_3).$$

.

$$X_n[i]=R*\cos(ang_1)* \cos(ang_2)..... \cos(ang_{n-1})* \cos(ang_n).$$

The text size generated by for said multi-bit text is given by n\*i. For example, if the number

of bits obtained from a coordinate is 20, the text size is  $n*20$ .

As referred to above, the above technique for generating a multi-bit text also provides a sequence of text to be generated by incrementing the equations for point  $P(i)$  to give point  $P(i+1)$ . This enables a new security key to be generated from the old key. If this regeneration  
5 of the security key is maintained for each transaction, it is extremely difficult for a hacker to mimic the genuine user's identity, as any attempt to use a captured security key will result in a failed transaction.

The generation of the next point  $P[i+1]$  depends on point  $P[i]$  and the increments of angles,  $dangle[i]$ ,  $i=0,1,2,\dots,49$ . It should be noted the 'dangle' is simply an array label used to  
10 denote the increments of the angle. The parameters  $dangle[i]$  and  $P[0]$  determine all the subsequent points  $P[i]$  generated and consequently, these parameters  $dangle[i]$  and  $P[i]$  are stored in a protected manner, by both the code engine and by the user/client on said portable recordable medium .

Any appropriate recordable medium may be used including, but not limited to CD-R, CD-  
15 RW, DVD-RW, USB key, flash card, floppy discs, memory card, smart chips and the like.

Although the user and the code engine may generate a 1000 bit text (for example) by virtue of the above mathematical technique, it would nevertheless be insecure for the user to transmit the text to the code engine for verification during a transaction. Therefore, before any transmission of the security key occurs during a transaction, the multi-bit text is further  
20 secured by application of said second encoding factor.

According to a preferred embodiment of the invention, said second encoding factor is a *hash function*. Hash Functions take a block of data as input, and produce a HASH as output. The usual intent is that the hash can act as a signature for the original data, without revealing its contents. Therefore, it is important that the hash function be irreversible - not only should it  
25 be nearly impossible to retrieve the original data, it must also be unfeasible to construct a data

block that matches some given hash value. However, HASH function are not random and are in fact completely deterministic, i.e. given the exact same input twice, the HASH function will always produce the same output. The HASH value should be small enough to be manageable in further manipulations, yet large enough to prevent an attacker from randomly  
5 finding a block of data that produces the same HASH.

A *hash function*  $H$  is a transformation that takes an input  $m$  and returns a fixed-size string, which is called the hash value  $h$  (that is,  $h = H(m)$ ). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography, the hash functions are usually chosen to have some additional properties.

10 The basic requirements for a cryptographic hash function are as follows.

- ξ The input can be of any length.

- ξ The output has a fixed length.

- ξ  $H(x)$  is relatively easy to compute for any given  $x$ .

- ξ  $H(x)$  is one-way.

15 ξ  $H(x)$  is collision-free.

A hash function  $H$  is said to be *one-way* if it is hard to invert, where "hard to invert" means that given a hash value  $h$ , it is computationally infeasible to find some input  $x$  such that  $H(x) = h$ . If, given a message  $x$ , it is computationally infeasible to find a message  $y$  not equal to  $x$  such that  $H(x) = H(y)$ , then  $H$  is said to be a *weakly collision-free* hash function. A *strongly*  
20 *collision-free* hash function  $H$  is one for which it is computationally infeasible to find any two messages  $x$  and  $y$  such that  $H(x) = H(y)$ .

Although there are several hash variants, one particular standard widely acknowledged

(particularly for digital signatures) as being highly secure is the SHA Hash function (or SHA-1) designed by National Standard and Technology Bureau of American and National Security Bureau of American.

This hash function *SHA* produces 160 bit hash outputs, i.e. a 160 bit hash text *h*, if  
5  $h=SHA(M)$ , where *M* is a text with more than 160 bits, and text *h* with 160 bits is the result converted by the *SHA* Hash function. Attacking the one-directional hash function *SHA* is dependant on the complexity of the task of finding a text *M'* such that  $SHA(M)=SHA(M')$ . The complexity of the attacking is  $O(2^{160})$  or approx 1.5EXP48. (ref. Bruce Schneier. Applied Cryptography.-Protocols, Algorithms, and Source Code in C).

10 As discussed above, according to said first encoding factor algorithm described above, a point on a 50 dimensional sphere generates the 1000 bits text. The calculation of the next point  $P[i+1]$  (performed for each transaction to regenerated a new security key) is based on the previous adjacent point  $P[i]$ , and the increments of the angles  $dangle[i]$ ,  $i=1,2,...49$ .

There are therefore two main ways for a hacker to attempt to fraudulently generate the next  
15 security key; -

- Firstly by calculating the previous point from its existing security key. This requires that the hacker knows the first encryption step algorithm and the parameters  $dangle[i]$ . However, to find the previous point  $P[i]$  from an existing security key based on a point  $P[i+1]$  involves attacking the SHA one-direction hash function with its complexity of  
20  $O(2^{160})$  permutations. Thus, even a computer capable of 1,000,000 sampling operations per second would takes approximately  $10^{40}$  years to complete the attack. Furthermore, since *M'* is not unique, even if the hacker is able to find a solution point by attacking SHA hash function successfully, the calculated point is not necessarily correct.

25 - Secondly, a hacker may steal the security key. Using enumeration strategy to find the

corresponding point  $P[i]$ , the hacker must also know the algorithm and parameters, and take  $O(2^{1000})$  to complete the algorithm. Since multiple values of  $M$  may produce the same  $h$  by the hash function  $h=SHA(M)$ , even if the hacker can obtain a value of  $M'$  that satisfies  $h=SHA(M')$ , the value of  $M'$  obtained does not necessarily represent the correct previous point.

It can be seen therefore, even if a hackers steals a security key, it is impossible to predict the next security key even if said first encoding algorithm was known to the hacker.

In a typical application of the invention, said transactions are online electronic funds transaction between a user, at least one seller and a bank.

Preferably, said security system further includes an additional password-based user-identification including an alphanumeric string to confirm the identity of a user by the code engine of the system.

In use, a client user of said security system is initially provided with a security key as follows;

- the client accesses a terminal of some form (e.g. a PC, bank terminal, dedicated terminal/card reader or the like) capable of interfacing and/or recording information on said portable recordable means,
- the client's user ID and/or password is passed via a secure network connection to a server coupled to said code engine,
- after authentication of the user ID and password, the code engine randomly generates the initial parameters for input to said first encoding algorithm and thereupon creates a first key code,
- wherein the security key is supplied to said client via the secure network connection for recording on said portable recordable medium, said server having retained a record of the security key.

A subsequent security key is generated and supplied to the client by said code engine after successful authentication of a client following application the client's password and existing security key through said secure network connection.

The security benefits of the above described security key may be enhanced by virtue of the medium on which the key is stored. According to one embodiment of the invention, said  
5 portable recordable medium is included in a multi-media multipurpose business/ID card. Such cards enable the storage of updateable printed and audio-visual information in combination with the security authentication role as described above. The card may be used it in many ways such as a conventional business card, loyalty card, brochures/catalog folio,  
10 video presentation, prepaid card and so forth.

An alternative, though equally innovative means of incorporating the security in a device already widely carried by individuals is through integration with a mobile/cellular phone. By utilising a short-range bi-directional RF transmitter such as an RFID unit within the business card or phone, it is possible to still further enhance the inventions effectiveness.

15 RFID is a short-range bi-directional RF transmission system (operating at 134.2 kHz or 13.56 MHz) with a range of applications including transportation (e.g. toll booth payment/ID authentication), asset management (e.g. airport baggage tracking, parcel delivery), access control (e.g. employee badges for corporate campuses), and user validation (e.g. electronic ticketing, automotive anti-theft systems).

20 A basic RFID system consists of three components:

- An antenna or coil
- A transceiver (with decoder)
- A transponder (RF tag) electronically programmed with unique information

The antenna emits radio signals to activate the tag and read and write data to it. Antennas are

the conduits between the tag and the transceiver, which controls the system's data acquisition and communication. Antennas are available in a variety of shapes and sizes; they can be built into any convenient object or at a particular location. The electromagnetic field produced by an antenna can be constantly present when multiple tags are expected continually. If constant  
5 interrogation is not required, the field can be activated by a sensor device.

Often the antenna is packaged with the transceiver and decoder to become a reader (a.k.a. interrogator), which can be configured either as a handheld or a fixed-mount device. The reader emits radio waves in ranges of anywhere from a few centimetres to 25 meters or more, depending upon its power output and the radio frequency used. When an RFID tag passes  
10 through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit (silicon chip) and the data is passed to the host computer for processing.

Thus, incorporation of an RFID unit with the security key authentication of the present invention provides 3 Primary Usages

15           ξ   Secured Multi-level Authentication for Online Access

              ξ   Contactless Payment and Loyalty Point Reward System

              ξ   Secured automated video advertisements/information delivery, update and billing transactions storage system.

A RFID unit or similar enables the realisation of so called 'M-payment' (mobile payment),  
20 i.e. a point-of-sale payment made through a mobile device, such as a cellular phone, smart phone smart card/smart chip or a personal digital assistant (PDA). Using M-payment. permits a user with a wireless device to pay for items in a store or settle a restaurant bill without interacting with any staff member.

Thus, a diner anxious to leave a restaurant for an appointment, the bill could be paid directly  
25 from the table - without waiting for the presentation of a physical bill. The user would simply

connect to the cash register with a wireless device, punch in the table number and bank personal identification number (PIN), and authorize payment. By utilizing the two stage security key authentication of the present invention, the risk (both perceived and actual) involved in such a transaction would be substantially ameliorated.

- 5 Other alternative like DNA marking/verification, finger print identification, voice print, cornea identification, facial recognition etc. can be similarly applied herewith to achieve as mentioned before to further enhance the inventions effectiveness.

It will be appreciated that the alternative portable recordable means to CD-R, CD-RW, DVD-RW, USB key, flash card, floppy discs, memory card, smart chips will become available over  
10 time. and will be capable of adaptation and incorporation into the present invention.

In yet further embodiments, the present invention may be used in dynamic authorisation including public key encryption. This dynamic authorisation may be performed in either of two modes, i.e. with or without the need to write the security code to said portable recordable medium.

- 15 Several advantages for both modes may be discerned.

Advantages/characteristics of the non-recording mode include:

- a. The ability to use the widespread conventional CD-ROM Drives or other CD-ROM compatible drives such as DVD or DVD-R/RW drives;
- b. The security key generated for authentication in each successive session is not  
20 sequential (as previously described in previous embodiments) but is randomly generated by server side upon initiating an authentication process (as described in more detail below);
- c. The ability to use known Secure Encryption techniques such as Diamond or Triple DES on both the Public and private security key parameters, with (optional)

additional security of protecting these parameters with a PIN known only to the user;

- d. The use of extended data length (1000 bit) and HASH encryption for validation/authentication.
- 5 e. Data Encryption: Any data may also be encrypted using the said known techniques during the process of transmission, with the public security key parameters as the key.

The recording mode also exhibits the same advantages/characteristics as above with the exception of points a) and b), which differ as follows:

- 10 a. A recordable medium (e.g. CD-R or CD-RW) is used to store the security key parameters data and PIN.
  - b. Successive security key parameters for authentication are generated sequentially (i.e. the new session parameters are derived from the previous security key parameters, as described for previous embodiments).
- 15 In both the recording and non-recording modes, the data integrity may respectively be validated via the 160 bit security key Hash Value of the 1000 bit text unique to the security key's pre-determined sequence of parameters (recording mode) and that unique to the transmitted Session and the security key Session Random Number generated by the server-side (non-recording mode).
- 20 The public security key parameters are derived in the same manner as described previously with the exception that they are generated for public usage for both the client and server side for use as a Public Encryption Key for known encryption methods such as Diamond, DES and so forth.

The private security key parameters are uniquely generated for each user in the same manner

as previously described and permit authentication of the user or transaction confirmation.

The secure encryption (e.g. Triple DES) on both the public and private security key parameters are protected by assigning a PIN to the user's smart card (or similar) storing the security key. Different variations of PIN configuration may also be implemented to enhance  
5 security, e.g. increasing the number of PIN digits, by adding 1,2,3 to the front or back of the PIN and based on a predefined format relative to the date or day of access, the user will key in the relevant sub-number i.e. 1,2,3 etc, and through an algorithm it will validate the sub-number before unlocking the security key card.

Therefore, according to one embodiment of the present invention, said security key  
10 parameters are protected via a client PIN, preferably located on said portable storage medium.

In use, the dynamic authentication non-recording mode operates as follows:

1. A user initiates a transaction by opening a login page of the security system server, which creates a 'Login Session ID'. It also generates a Dynamic Public Security Key (DPSK) which is encrypted by known strong encryption means  
15 using a Public Security Key (PSK) and returned to the client-side application.
2. Optionally, the Client is prompted for their PIN identification for further access
3. After successfully PIN entry, the client application will decrypt the Dynamic Public Security key using the Public Security Key sent via the server.
4. Thereafter, the server will generate a Session Random Number (SRN), which is  
20 the dynamically generated parameter value to be used in the security key's first encoding factor. The SRN is encrypted with the known strong encryption with Dynamic Public security key (DPSK) and sent back to the client's application.
5. The client's application will then display the Portal login Screen to the secure website and prompts the User to input a Login ID and Password.

6. The correct user input causes the Client's application to:-
  - a. Decrypt the received data from Server using the DPSK to obtain the SRN;
  - b. generate the Session security key code (1000 bit) based on the SRN and the Private Security Key parameters (PSKP) and hash it to produce a 160 bit Session Hash Value (SHV);
  - c. use strong encryption to encrypt a data string including the SHV, SRN, ID/Password and CardID using the DPSK and transmit the encrypted data to the server.
7. Upon receipt, the server decrypts the data using the DPSK. Based on the CardID, it will validate the submitted ID/Password before the server retrieves the user's PSKP and generates the SHV using the received SRN.
8. After generating the Server-side's SHV, it is compared with the received Client-side's SHV in order to verify the Security key authentication is successful.
9. If verification is achieved, access for the client's terminal to the secure website is granted. The transaction time and details are also logged by the security server.
10. Data Encryption:

In addition to the above user identification/authentication process, any other transmitted data may be encrypted using the strong encryption with the DPSK as the key. Moreover, the data integrity may be checked by validating the SHV value unique to the transmitted Session and the SRN generated by the server-side.

It can be seen therefore that the session generated Security key does not require recording on the user's portable storage medium such as via a CD-RW card.

Therefore, according to a further embodiment, the present invention further provides dynamic

authentication of a user utilising public key encryption of data exchanged between the user and said security system.

Preferably, said public key encryption includes a public key comprised of said security key parameters uniquely generated for public usage by the security system and one or more client  
5 users, and private security key parameters.

It will be appreciated that reference to a 'client' herein is used to incorporate the client-side software and hardware necessary to provide an on-line network interface and to perform client-side applications

Preferably, for each user transaction session,

- 10 - said security system generates a dynamic public security key and transmits same to the client after encryption using said public key;
- the client decrypts said dynamic public security key using the public key sent from the security system;
- the security server generates a transaction session random number corresponding to  
15 said security key parameters and transmits same to the client after encryption using said dynamic public security key;
- said client decrypts said transaction session random number using the dynamic public security key and incorporates same into said first encoding factor of the security key to produce a transaction session multi-bit text;
- 20 - said second encoding factor is applied to the session multi-bit text and the resultant is encrypted before being sent to said security server;
- the security server decrypts the received data before determining validation of said authentication by comparing with a security key generated from the application of

said first and second encoding factors to said private security key parameters stored in said security system.

In comparison, the dynamic authentication recording mode operates as follows:

1. A user initiates a transaction by opening a login page of the security system server, which creates a 'Login Session ID'. It also generates a Dynamic Public Security Key (DPSK) which is encrypted by known strong encryption means using a Public Security Key (PSK) and returned to the client-side application.
2. Optionally, the Client is prompted for their PIN identification for further access
3. The client's application will then display the Portal login Screen to the secure website and prompts the User to input a Login ID and Password.
4. The correct user Login ID and Password input causes the Client's application to:-
  - a. generate the User security key code (1000bit) based on the Sequential User's Private Security Key parameters (PSKP) and hash it to produce a 160 bit User Hash Value (UHV).
  - b. use strong encryption to encrypt a data string including the UHV, ID/Password and CardID using the DPSK and transmit the encrypted data to the server.
5. Upon receipt, the server decrypts the data using the DPSK. Based on the CardID, it will validate the submitted ID/Password before the server retrieves the user's PSKP and the last stored sequential parameters of the User's security key code and generate the UHV.
6. After generating the UHV, it is compared with the received Client-side's UHV in order to verify the Security key authentication is successful. If verification is successful, it will store the subsequently generated Dynamic Security Key

Parameter Value (DSKP) back to the security server's Database. It will transmit the successful validation back to the clients.

7. If verification is achieved, access for the client's terminal to the secure website is granted. The transaction time and details are also logged by the security server.
- 5 8. On the client-side the application will increment the next parameter value of the DSKP) and stored it on to the user's security key portable recordable storage medium.
9. Data Encryption: Again, in addition to the above user identification/authentication process, any other transmitted data may be encrypted using the strong encryption  
10 with the DPSK as the key. Moreover, the data integrity may be checked by validating the UHV value unique to the transmitted Session and the SRN generated by the server-side.

Thus, this mode utilizes the previously described means of successively generating the security key parameters and transmitting them between the client and security server and  
15 enables the use of public key encryption for both the security key parameters and user ID details.

Thus, according to an alternative embodiment, the present invention provides dynamic authentication during each user transaction session wherein,

- said security system generates a dynamic public security key and transmits same to  
20 the client after encryption using said public key;
- the client decrypts said dynamic public security key using the public key sent from the security system and generates a multi-bit text from the client's existing stored private security key parameters by applying said first and second encoding factors before encrypting the resultant data and sending to the security system;

- the security server decrypts the data using the dynamic public security key and compares with the result of applying the first and second encoding factors to the private security key parameters stored in the security system to verify successful authentication;
- 5 Preferably, if said verification is successful, the next dynamic security key parameter is stored on the security server, while the client application also increments the dynamic security key to store the parameters of the next point.

If a disk, inserted in a diskette drive (or similar) of a computer, is used for a transaction, the code contained on the disk is read by the security system operable when a transaction is  
10 occurring.

The 'A' drive is the usual name accorded a diskette drive reader of a computer. It will be appreciated that such drives may be mapped with an alternative letter on a computer.

The code on the disk permits a central server or engine to authenticate the code and confirm this with the software of the seller and any bank involved. The code, when later used to  
15 confirm the transfer of funds for payment, can also be used to update the records of the buyer with the bank, and to update the records with the seller for the generation of billing.

In accordance with this invention the machine readable disk may be of the standard type of 3 1/4 inch disk that can be easily carried in a pocket, bag, etc, and is personal to the buyer, not limited to the computer or internet connection on which the buyer is conducting the  
20 transaction.

The code on the disk may be of many types and may involve one or more elements. Each time the code is used one or more elements may be changed. For example, to create starting codes for a user, four random numbers may be generated. Two of these numbers can be five digit numbers which can be merged to a ten digit number as a user starting code. With this  
25 number and the code, every user is assigned three numbers or parameters that are used for

modifying the user code. The three parameters vary from user to user.

When a user uses the system, the code of the user is modified. The modification will be in two parts; one part for a significant change and another part to avoid repetition.

The code in each disk for each user is made up of a string of code and additional dummy  
5 codes and scrambled or encrypted into a key or code. The encryption is only accessible and readable by the code engine. A code of 10 kb in data size is preferable for ease of speed of reading and life span of the disk.

In addition to this the disk can be monitored for unauthorised duplication. For example, if the code on the disk is being duplicated to (for example, 10 copies) once one of the duplicated  
10 disks or the original disk is being used for any transaction, a new code will be rewritten within the original disk for the next transaction. This rewritten code becomes the valid code. Thus the remaining 9 copies, which include the original code of the original disk, will be voided and invalidated for any subsequent use with the code engine.

Additionally, as another example, limits can be set within the code for copying of the code,  
15 so that after a set number of copies (for example, 9) the original and all further copies may be voided and invalidated for use.

Appropriate monitoring, of known type, at the code engine site can also be used to ascertain whether invalid disks with duplicate codes are being used. The transaction can be invalidated or provide an audit trail for forwarding to appropriate authorities.

20 In accordance with this invention the security system may further include a password-based user identification system, operable through the internet interfaces, which may be further used to identify a buyer to the system. The password as used herein is a string of symbols, which are used to authenticate an identity as additional to, or part of, the above security system.

An alternative to a password can be a system whereby the user controls the validation process by allowing the user to set personal security levels or on or off controls to activate or deactivate validation processes in conjunction with the valid code on the disk.

Such controls can be used for other purposes as well, for example, to inactivate the code for a period of time when aspects of the user's system will not be in operation (for example, inactivating a credit card for use for internet transactions).

### **BRIEF DESCRIPTION OF THE DRAWINGS**

The present invention can more fully be understood by reference to the following detailed description and accompanying drawings, which form an integral part of the application.

Figure 1. is a pictorial representation of the flow system using the security system according to a first embodiment of the present invention; and

Figure 2. is a pictorial view of an application of the security system according to a first embodiment of the present invention in a real time setting of a library;

Figure 3. is a schematic representation of a system for distribution of a security key according to said second embodiment of the present invention;

Figure 4. is a schematic representation of a system for authentication and regeneration of a security key according to said second embodiment of the present invention;

Figure 5. is a further schematic representation of a system for authentication and regeneration of a security key utilising a smart card according to said second embodiment of the present invention;

Figure 6. is a representation of a 50-dimensional sphere in accordance with a second embodiment of the present invention;

Figure 7. is a representation 2-dimensional circle, and

Figure 8. is a representation 3-dimensional sphere.

Figure 9. is a schematic representation of a system for dynamic authentication and regeneration of a security key according to a further embodiment of the present invention;

## 5 DETAILED DESCRIPTION

Figure 1 illustrates the system in accordance with a first embodiment of the present invention. A portal server 1 incorporates an electronic engine 2 for the generation and checking of codes. The engine 2 incorporates appropriate software for identifying and reading codes forwarded electronically to it, or to the portal, and for identifying such codes and providing  
10 code authentication. The portal 1 and the engine 2 form part of the internet or web 3, which can be connected to by one or more PCs 4 representing the computer being used by one or more end users 5. Each user 5 has a disk with a code 6 thereon. Each user 5 has received the code 6 after application to the service provider operating the portal 1 and engine 2.

The disk with code 6 is forwarded to the user 5 by non-electronic means, after application by  
15 the user 5 for such a code 6. The user 5 may be an end retailer, or e-retailer. The user 5 may be a business in a supply chain who is placing orders for goods electronically in a B2B situation. Whilst the method of connection to the internet 3 has been represented as PC computer 4, it will be appreciated that any other form of internet connection, with means for machine reading of disks, may be used without departing from the scope of the invention.

20 The code 6 may be copy-protected by a number of means before being forwarded to the user 5. In addition to this the disk can be monitored for unauthorised duplication. For example, if the code 6 on the disk is being duplicated to (for example) ten copies, once one of the duplicated disks or the original disk is used for any transaction, a new code will be rewritten within the original disk for the next transaction. This rewritten code becomes the valid code  
25 6. Thus the remaining nine copies, which include the original code of the original disk, will

be voided and invalidated for any subsequent use with the code engine 2.

As an alternative, and if so desired, the disk with code 6 is incorporated with safe guards that erase the original after a specified number of times the disk has been copied – for example, nine times.

5 In addition to this security measure, the portal 1 and engine 2 can incorporate programming for comparison in order to ascertain whether or not two different people are using the same codes, the code having been copied. In the event that a copied code is used the portal 1 and engine 2 are pre-programmed such that an audit trail can be monitored or reproduced if needed by the appropriate authorities.

10 As an example of the operation of the invention: the user 5 selects and places an order with an e-commerce seller 7. The company 7 advises the user 5 of the billing requirements and asks for code authorisation and authentication. The user 5 provides this to the engine 2 by a code handshake and authentication (9, 10). The engine 2 will only provide code authentication 10 if the code 6 is present in the 'A' drive of PC 4 of the user 5. Once the code  
15 authentication 10 is provided the user 5 can also provide authorisation for payment. The ability to effect payment requires an electronic query by the bank 12 in question, who also use code authentication 13 for payment status 14. This payment is cleared through the banking system via route (13 and 14) as shown on Figure 1. The user 5 can verify billing, selection and settlement 8 and payment status 11 during code verification 13.

20 The portal 1 and engine 2 are preferably operated by an independent administrator or business 15. The codes 6, on disks, can be issued on individual application to the business 15. Alternatively the business 15 can bulk issue codes on disks to an appropriate further business 17 (which may be a bank 12). With appropriate backups for example an escrow agent 16, the system can be varied as is required by the businesses 7, banks 12 and users 5, or a  
25 combination thereof.

It will be appreciated that with the use of an independent body 15 a multiple number of computing companies in the same field (for example the banking industry) would be able to use the system of codes 6 with confidence.

Each company 7, when electronically billing, can generate billings and records of other  
5 transactions 18, which are then collated and /or consolidated 19 for each user 5. These collated transactions 19 are forwarded via portal 1 to either the bank 12 or end user 5, as directed. The user 5 can instruct the relative bank 12 by use of the code 6 to pay the account, or have standing instructions to the bank 12. The bank 12 uses the code authentication 13, payment status 12, and payment clearance 14 query to transfer funds to meet the account.

10 The portal 1 and engine 2 can be programmed to permit an additional layer of security. For example a password could be used to further authenticate the access of the user 5. Such coding could be used in addition to or as a temporary replacement for the code 6 on the disk if it were, for example, lost or misplaced.

A further, additional layer of security can optionally be added. This can be separate from the  
15 code 6 on a disk and with or without any password as described above. The control of such system would still lie with the user 5 of the disk. The additional layer of security would be a 'flag control' 29 operable by the user 5. Such flag control 29 can be used by the user 5 to activate or deactivate a validation process such that the code 6 on the disk and or password are secondary validation procedures.

20 Examples of the operation of such control can include, for example, the deactivation of a particular style of transaction 18 by the user 5; for example: credit card or mobile phone 24 for a specified period of time or indefinitely.

This can be of a advantage if a credit card is used on the internet and then the card is lost as it will prevent anyone illegally using the credit card of the user 5 for any transaction 18 on the  
25 internet.

Methods of setting such controls can include but are not limited to:

- a stipulated SMS message incorporating the valid password to set the control and record it through the portal 1 with the engine 2;

- a phone call using an automated keypad 25 answering service to note the user 5 and password via the keypad 25 before setting this control;

- via the internet using SSL encryption and the valid ID and password to log in and activate the control page through the portal 1 and engine 2, to set the control; and

- other communication media that can link to the internet and include keypads 25 and alpha numeric pads (including, for example, other WAP applications).

10 According to the first embodiment of the invention as described with reference to figures 1-2, a first key generation algorithm is now described.

The code 6 is generated in, for example, ten digits with a unique number for each of every 100,000 users 5. Every time a user 5 uses the invention the code is modified. The starting code 6 for each user 5 is four random numbers. From the four random numbers two numbers, 15 each of which are five digit, are merged to create a ten digit number. With this number every user 5 is assigned three numbers or parameters that are used for modifying the starting code 6. The parameters are different for each user 5. As the user 5 uses the invention, the code 6 must be modified. It is obvious that a different number is required and that this number is not often repeated. To achieve this two of the three parameters operate to change the code. One 20 of the parameters is for a significant change and the another parameter is to avoid repetitions. Thus each of the parameters rotates to generate different numbers within the numeric code 6.

The code 6 on the disk is comprised of the actual string of code and additional dummy codes which are scrambled or encrypted. The actual string of code 6 is broken up to seven sub-strings before being scrambled with those generated dummy codes. to form a code of

approximately 10 kb in data size. It is not desirable to have the size of the code any larger than this, as reading it would otherwise take too much time.

Referring to Figure 2, the real time example given for the operation of the system described with reference to the first embodiment shown in figure 1 is the operation of a library with a web-server 21, and in relation to customers 35 wishing to read from a selection of e-books held on a master database 36. Customers 35 query through the internet 22 and web-server 21 those books they wish to read or view. These books can be electronically downloaded as HTML pages 27 from the master database 36. The system can query the customer 35 for code for verification (which uses the disk and code 6 of Figure 1) and the charge for the download recorded in the payment manager 26.

It will be understood that by appropriate regular billing, the individual charges recorded by the payment manager 26 can be itemised on an electronic account and forwarded to the customer 35. Via the system outlined in Figure 1, the customer 35 may review the account and authorise the payment through his or her bank 12 with the aid of the code 6 on their personal disk.

Whilst the above described system has been discussed with use of the internet, it will be appreciated that this could also incorporate an intranet, and input means can be any connecting means capable of connection to the Internet an incorporating an 'A' drive.

The invention will now be described with reference to further embodiments as shown in figures 3-8.

In these embodiments, the present invention relates to a system and method for authenticating transactions conducted over a network, particularly the internet, utilising a high security code engine generating self morphing security key codes, which may be stored by the user in a convenient recordable medium.

Regarding figures 3, a security system 100 is there shown comprised of ; a user or client 101,

accessing a terminal 102, through a portable recordable medium in the form of a smart card 103, linked via a network such as the internet 104 to a security key server 105 incorporating a code engine 106, in communication to a database 107. It will be appreciated the configuration shown in the figure 3 is but one of numerous configurations.

5 Figure 3 illustrates the procedure for the initial issuing of a security key code to the client 101. The client 101 inputs their smart card (which also acts as a CD-RW multipurpose business card) into an appropriate drive in the terminal 102 and sends a request (together with the user ID and password of the client 101) for the issuance of a security key code to the security key server 105 via a secured network 104.

10 In turn the security key server 105 passes the client ID information and security key request to the code engine 106. A unique key is then generated using a two factor encoding algorithm as described in more detail below. The algorithm utilises the client's user ID/password information in the security key generation process. The code engine 106 stores a copy of the newly generated security key in the database 107 and also sends another copy back to the  
15 client 101 via the secure network 103 to be recorded on the smart card 103 in the terminal 102.

The client is then free to carry their smart card 103 with them until they next desire to perform a transaction requiring user authentication of some form. Typically, this will be a financial transaction whereby the client 101 wishes to purchase a service or product and pay  
20 for it electronically online. It should be noted however that the security key may be used to indicate the authenticity of a variety of communication aside from financial transactions.

Figure 4 shows a schematic representation of the scenario where the client 101 undertakes a online financial transaction via the internet 104. Figure 4 shows additional elements and connections to those shown in figure 3 including;

25 - an internet web server 108 connected to the client terminal 102;

- a bank server 109 in two-way communication with the web server 108 via a secure connection 110 employing a secure protocol such as SSL, and a one way transmission connection to the security key server 105;
- and respective firewalls 111 for the security key server 105, web server 108 and bank  
5 server 109 each acting as an interface with all incoming and outgoing communications with the respective servers; and
- security key server 105 is also configured to transmit (but not receive) data to the web server 108.

The client 101 logs onto the webserver 108 via their user terminal 102 (which may be a home  
10 PC, a cybercafe terminal, a store customer terminal and so forth) after connecting their smart card 103 to an appropriate interface with the terminal 102.

The client 101 is then prompted for their user ID and password which is received through the firewall 111 of the web server 102. The clients identification details are then submitted for verification at the bank server 109 and if successful, the client identification details plus send  
15 their existing security key code is sent via the bank web server 109 to the security key server 105.

Verification of the security key is then performed by the code engine 106 and checked with that stored in the database 107. If successful, a new security key code is generated and this information is sent back to the client 101 via the secure network to update the security key  
20 code held in the client's smart card 103.

If at any point the user ID/password or security key code authentications fail, the client 101 is advised accordingly and prevented from accessing any further services.

It can be thus seen that every user transaction updates the security key code thereby avoiding the risk of a hacker capturing details of the transaction and subsequently presenting

themselves as the genuine user.

As referred to above, the client 101 need not necessarily use a CD-RW smart card 103 and may alternatively employ some form of DVD-RW media, USB keys, flash cards, floppy discs, or the like.

5 Figure 5 shows a range of communication means by which the client may conduct a secure transaction with authentication according to the present invention. In addition to the use of client terminals 102, a client 101 may use one of several merchant facilities provided for customers including a dedicated merchant access terminal 113 or a specialised reader 114 for the smart cards 102, attached to each participating point of sale (POS) outlet 114. The POS  
10 terminals 114 may be connected to a clearing house of bank 109 of some form via numerous connection means such as cable, a dial-up connection, DSL etc.

In the embodiment shown in figure 5, both the POS terminal 114 and the user/customer terminals 102/113 are connected (via the financial clearing house 109 and the internet 104 respectively) to a smart card “gateway” 116. This gateway 116 is effectively a collection of  
15 servers operating various methods commerce transactions including: an eCoupon promotion server 117, an advertising server 118, a customer loyalty program server, an eCommerce gateway (merchant virtual store) 120 and an mPayment server 121.

It will be appreciated that the different servers represented in the smart card gateway are given by way of example only and the invention is not limited to same. Incorporation of a  
20 RFID unit (not shown) into the smart card 103 or even into another readily available and transportable such as mobile phones or personal accessories/devices e.g. pens, watches, music players (radio, MP3 players) and the like increases the wider application of the security system. It furthermore increases the likelihood of the user having the necessary secure transaction authentication hardware (e.g. the smart card, or RFID enabled device) on their  
25 person when engaged in general daily activities and not requiring any user assessment/prediction of whether the security specific card may be needed.

In the second embodiment as described above with reference to figures 3-5, the invention utilises a security key code generated by an algorithm with two encoding factors. These factor are the creation of a multi-bit text (preferably a 1000 bit) as described below, followed by applying a hash function to the text.

5 The first encoding factor comprising a multi-bit text is obtained from the co-ordinates on a multi-dimensional sphere 122 (illustrated in figure 6) of a point P(i) 123. A subsequent point P[i+1] 124 on the surface of the sphere 122 is related to the previous point P(i) 123 according a defined mathematical relationship. This enables a series of security codes to be generated upon each transaction.

10 The concept of using points on the surface of a multi-dimensional sphere is difficult to illustrate though mathematically derivable by a direct extrapolation of the geometric relationships involved in simple 2 and 3 dimension equivalents, i.e. a circle and sphere.

The parameter equation of a circle 125 (as shown in figure 7) is

$$y=R*\sin(\text{ang}).$$

15  $x=R*\cos(\text{ang}).$

where the parameter 'ang' 126 denotes an angular value from 0 to 360<sup>0</sup>.

The shape transcribed by the point (x,y) 127 through the full parameter range is a circle.

The parameter equation of a sphere 128 (shown in figure 8) is:

$$z=R*\sin(\text{ang}_1).$$

20  $y=R*\cos(\text{ang}_1) * \sin(\text{ang}_2).$

$$x=R*\cos(\text{ang}_1)* \cos(\text{ang}_2).$$

where its parameters ang<sub>1</sub> 129 and ang<sub>2</sub> 130 vary from -90<sup>0</sup> to 90<sup>0</sup> and from 0<sup>0</sup> to 180<sup>0</sup> respectively.,

The shape transcribed by the point (x,y,z) 131 through the specified parameter range is a

sphere.

It can be thus seen that a multi-dimension sphere is an extension of the parametric equations in two and three-dimensions.

Consequently, for an 'n' dimensional sphere may be represented by the equations said

5 co-ordinates  $P(i) = (x_1[i], x_2[i], x_3[i], \dots, x_n[i])$  are given by

$$x_1[i] = R \cdot \sin(\text{ang}_1).$$

$$x_2[i] = R \cdot \cos(\text{ang}_1) \cdot \sin(\text{ang}_2).$$

$$x_3[i] = R \cdot \cos(\text{ang}_1) \cdot \cos(\text{ang}_2) \cdot \sin(\text{ang}_3).$$

.

10

$$X_n[i] = R \cdot \cos(\text{ang}_1) \cdot \cos(\text{ang}_2) \cdot \dots \cdot \cos(\text{ang}_{n-1}) \cdot \cos(\text{ang}_n).$$

As referred to above, the above technique for generating a multi-bit text also provides a sequence of text to be generated by incrementing the equations for point  $P(i)$  123 to give point  $P(i+1)$  124.

15 The generation of the next point  $P[i+1]$  124 depends on point  $P[i]$  123 and the increments of angles  $\text{dangle}[i]$ ,  $i=0,1,2,\dots,49$ . The parameters  $\text{dangle}[i]$  and  $P[0]$  determine all the subsequent points  $P[i]$  123 generated and consequently, these parameters  $\text{dangle}[i]$  and  $P[i]$  are stored in a protected manner, by both the code engine and by the user/client on said portable recordable medium .

20 In yet further embodiments, the present invention may be used in dynamic authentication including public key encryption. This dynamic authentication may be performed in either with or without the need to write the security code to said portable recordable medium.

In both the recording and non-recording modes, the data integrity may respectively be validated via the 160 bit security key Hash Value of the 1000 bit text unique to the security  
25 key's pre-determined sequence of parameters (recording mode) and that unique to the transmitted Session and the security key Session Random Number generated by the server-

side (non-recording mode).

The public security key parameters are derived in the same manner as described previously with the exception that they are generated for public usage for both the client and server side for use as a Public Encryption Key for known encryption methods such as Diamond, DES  
5 and so forth.

The private security key parameters are uniquely generated for each user in the same manner as previously described and permit authentication of the user or transaction confirmation.

The secure encryption (e.g. Triple DES) on both the public and private security key parameters may be optionally protected by assigning a 6 digit PIN to the user's smart card  
10 103 (or similar) storing the security key. Different variations of PIN configuration may also be implemented to enhance security, e.g. increasing the number of PIN digits or by adding 1, 2, 3 to the front or back of the PIN and based on a predefined format relative to the date or day of access, the user will key in the relevant sub-number i.e. 1,2,3 etc, and through an algorithm it will validate the sub-number before unlocking the security key card.

15 Therefore, according to one embodiment of the present invention, said security key parameters are protected via a client PIN, preferably located on said portable storage medium.

In use, the dynamic authentication non-recording mode operates as follows (and as shown in figure 9, where stages I-VII correspond broadly to the like numbered points below):

- I. A user (not shown) initiates a transaction by opening a login page of the security system  
20 server (105), which creates a 'Login Session ID'. It also generates a Dynamic Public Security Key (DPSK) 132 which is encrypted by known strong encryption means using a Public Security Key (PSK) 133 and returned to the client-side application.
- II. Optionally, the Client is prompted for their PIN 134 identification for further access
- III. After successfully PIN 134 entry, the client application will decrypt the Dynamic Public

Security key (DPSK) 132 using the Public Security Key 133 sent via the server.

- IV. Thereafter, the server will generate a Session Random Number (SRN) 135, which is the dynamically generated parameter value to be used in the security key's first encoding factor, i.e generating a 1000 bit text from the parameters defining point P[i] 123 as given above . The SRN 135 is encrypted with the known strong encryption with Dynamic Public security key (DPSK) 132 and sent back to the client's application.

The client's application will then display the Portal login Screen to the secure website and prompts the User to input a Login ID and Password 136.

The correct user input causes the Client's application to:-

- a. Decrypt the received data from Server using the DPSK 132 to obtain the SRN 135;
- b. generate the Session security key code (1000 bit) based on the SRN 135 and the Private Security Key parameters (PSKP) 137 and hash it to produce a 160 bit Session Hash Value (SHV) 138;
- c. use strong encryption to encrypt a data string including the SHV 138, SRN 135, ID/Password 136 and CardID 134 using the DPSK 137 and transmit the encrypted data to the server.
- V. Upon receipt, the server decrypts the data using the DPSK 137 and validates the CardID 134 based on the submitted ID/Password 136.
- VI. The server retrieves the user's PSKP 137 and generates the Server-side's SHV 138 using the received SRN 135.
- VII. After generating the Server-side's SHV 138, it is compared with the received Client-side's SHV 137 in order to verify the Security key authentication is successful.

If verification is achieved, access for the client's terminal 102 to the secure website (not shown) is granted. The transaction time and details are also logged by the security server 105.

- 5    The DPSK 132 may also be used as the public key to encrypt other data for transmission .  
The data integrity may be checked by validating the SHV 137/138 value unique to the transmitted Session and the SRN 135 generated by the server-side.

In comparison, the dynamic authentication recording mode operates as follows (also described with reference to figure 9, where common elements to the above –describe  
10    recording mode are like numbered):

- I. A user initiates a transaction by opening a login page of the security system server, which creates a 'Login Session ID'. It also generates a Dynamic Public Security Key (DPSK) 132 which is encrypted by known strong encryption means using a Public Security Key (PSK) 133 and returned to the client-side application.
- 15    II. Optionally, the Client is prompted for their PIN identification 134 for further access
- III. The client's application 102 will then display the Portal login Screen to the secure website and prompts the User to input a Login ID and Password 136.
- IV. The correct user Login ID and Password input 136 causes the Client's application to:-
  - a. generate the User security key code (1000 bit) based on the Sequential User's  
20    Private Security Key parameters (PSKP) 137 and hash it to produce a 160 bit User Hash Value (UHV) 140.
  - b. use strong encryption to encrypt a data string including the UHV 140, ID/Password 136 and CardID 134 using the DPSK 137 and transmit the encrypted data to the server 105.

- V. Upon receipt, the server 105 decrypts the data using the DPSK 137. Based on the CardID 134, it will validate the submitted ID/Password 136 before the server retrieves the user's PSKP 137 and the last stored sequential parameters of the User's security key code and generate the UHV 139.
- 5 VI. After generating the Server-side's UHV 139, it is compared with the received Client-side's UHV 138 in order to verify the Security key authentication is successful.
- VII. If verification is successful, the subsequently generated Dynamic Security Key Parameter Value (DSKP) 132 is stored back to the security server's Database 107. The successful validation is transmitted back to the client application 102.
- 10 If verification is achieved, access for the client's terminal 102 to the secure website (not shown) is granted. The transaction time and details are also logged by the security server 105.

On the client-side the application increments the next DSKP 137 parameter value and stored it on to the user's security key portable recordable storage medium 103.

- 15 Thus, this mode utilizes the previously described means of successively generating the security key parameters and transmitting them between the client and security server and enables the use of public key encryption for both the security key parameters and user ID details.

- 20 Aspects of the present invention have been described by way of examples and it should be appreciated that the concept and principals of the system described are most important but also that modifications and additions may be made thereto without departing from the scope thereof.

## CLAIMS:

1. A security key for use in online transactions over electronic networks between users, said users including: at least one client, and at least one recipient, characterised in that each key, includes code generated independently from said client and recipient, characterised in that said code generation includes a first encoding factor wherein a multi-bit code text is at least partly formed from parameters derived from co-ordinates of a point  $P(i)$  on a multi-dimensional sphere.
2. A security key as claimed in claim 1, wherein for a sphere of 'n' dimensions, said co-ordinates  $P(i) = (x_1[i], x_2[i], x_3[i], \dots, x_n[i])$  are given by

$$x_1[i] = R * \sin(\text{ang}_1).$$

$$x_2[i] = R * \cos(\text{ang}_1) * \sin(\text{ang}_2).$$

$$x_3[i] = R * \cos(\text{ang}_1) * \cos(\text{ang}_2) * \sin(\text{ang}_3).$$

.

.

.

.

.

$$X_n[i] = R * \cos(\text{ang}_1) * \cos(\text{ang}_2) * \dots * \cos(\text{ang}_{n-1}) * \cos(\text{ang}_n).$$

3. A security system for transactions for use in user authentication and for confirmation of transactions over electronic networks said system including online processing of transactions between users, said users including: at least one client, and at least one recipient, wherein each transaction incorporates use of a unique security key as claimed in claim 1 or claim 2, wherein said system incorporates computer processor and memory means for generating each key, said key comprising: code generated independently from said client and recipient by a code engine, said code including said first encoding factor and at least one further encoding factor.

4. A security system as claimed in claim 3, wherein said key is regenerated upon each transaction and is supplied to said user for storage in a portable storage medium.
5. A security system as claimed in claim 3, wherein a second encoding factor is applied to said multi-bit text of said first encoding factor; said second encoding factor comprising the application of a HASH algorithm.
6. A security system as claimed in claim 3, wherein said transactions are online electronic funds transaction between a user, at least one seller and a bank.
7. A security system as claimed in claim 3, wherein said multi-bit text is less than or equal to a 1000 bits and said multi-dimensional sphere is less than or equal to 50 dimensions.
8. A security system as claimed in claim 3, wherein said system further includes an additional password-based user-identification including an alphanumeric string to confirm the identity of a user by the code engine of the system.
9. A security system as claimed in claim 8, wherein said key is initially randomly generated by said code engine upon a request from the client following verification of said password-based user identification and then supplied to said client via a secure network connection.
10. A security system as claimed in claim 9, wherein a subsequent key is generated by said code engine after successful authentication of a client following application the clients password and existing key, whereupon a new key is generated and supplied to the client.
11. A security system as claimed in claim 4, wherein said portable medium is selected

from, but not limited to the group: CD-R, CD-RW or DVD-RW media, USB keys, flash cards, floppy discs, smart chip/card.

12. A security system as claimed in claim 11, wherein said portable medium is included in a multi-media multipurpose business card.
13. A security system as claimed in claim 11, wherein said portable medium is incorporated into a smart card.
14. A security system as claimed in claim 11, wherein said portable medium is incorporated into a mobile phone.
15. A security system as claimed in any one of claims 12-14, further incorporating a short-range bi-directional RF transmitter and it can also include item like DNA marking, finger print, voice print, cornea identification, facial recognition etc.
16. A security system as claimed in claim 15, wherein said transmitter is a RFID unit.
17. A security system as claimed in claim 3, wherein said regeneration of said key includes calculating co-ordinates of a further point  $P(i+1)$  on said multi-dimensional sphere.
18. A security system as claimed in claim 17, wherein said further point is determined by parameters  $P[0]$  and  $dangle[i]$ .
19. A security system as claimed in claim 18, wherein said parameters further include sphere radius  $R$ .
20. A security system as claimed in claim 3, wherein said parameters are stored and protected on said portable medium.
21. A security system as claimed in claim 20, wherein said security key parameters are

protected via a client PIN.

22. A security system as claimed in claim 5, utilising public key encryption of data exchanged between the user and said security system.
23. A security system as claimed in claim 22, wherein said public key encryption includes a public key comprised of said security key parameters uniquely generated for public usage by the security system and one or more client users, and private security key parameters.
24. A security system as claimed in claim 23, capable of providing dynamic authentication wherein for each user transaction session,
  - said security system generates a dynamic public security key and transmits same to the client after encryption using said public key;
  - the client decrypts said dynamic public security key using the public key sent from the security system;
  - the security server generates a transaction session random number corresponding to said security key parameters and transmits same to the client after encryption using said dynamic public security key;
  - said client decrypts said transaction session random number using the dynamic public security key and incorporates same into said first encoding factor of the security key to produce a transaction session multi-bit text;
  - said second encoding factor is applied to the session multi-bit text and the resultant is encrypted before being sent to said security server;
  - the security server decrypts the received data before determining validation

of said authentication by comparing with a security key generated from the application of said first and second encoding factors to said private security key parameters stored in said security system.

25. A security system as claimed in claim 23, capable of providing dynamic authentication wherein for each user transaction session;
  - said security system generates a dynamic public security key and transmits same to the client after encryption using said public key;
  - the client decrypts said dynamic public security key using the public key sent from the security system and generates a multi-bit text from the client's existing stored private security key parameters by applying said first and second encoding factors before encrypting the resultant data and sending to the security system;
  - the security server decrypts the data using the dynamic public security key and compares with the result of applying the first and second encoding factors to the private security key parameters stored in the security system to verify successful authentication;
26. A security system as claimed in claim 25, wherein if said verification is successful, the next dynamic security key parameter is stored on the security server, while the client application also increments the dynamic security key to store the parameters of the next point.
27. A method of authenticating the unique identity of a user for transactions over electronic networks, said system including online processing of transactions between users, said users including: at least one client, and at least one recipient, wherein each transaction incorporates use of a unique security key. characterised

in that the method includes:

- providing a security system incorporating computer processor and memory means on which is operated a code engine generating said codes,
- on application by a client, providing said key comprising: code generated independently from said client and recipient by a code engine, said code including at least a first and second encoding factors, said first encoding factor comprising a multi-bit code text at least partly formed from parameters derived from co-ordinates of a point P(i) on a multi-dimensional sphere.

28. A method as claimed in claim 27, further including the step wherein said key is regenerated and supplied to said client upon each successive and successful transaction application by the client.
29. A method as claimed in claim 28, further including the step wherein said key regenerated and supplied to said client is stored on a portable storage medium upon each successive and successful transaction application by the client.
30. A method as claimed in claim 27, wherein for a sphere of 'n' dimensions, said co-ordinates  $P(i) = (x_1[i], x_2[i], x_3[i], \dots, x_n[i])$  are given by

$$x_1[i] = R \cdot \sin(\text{ang}_1).$$

$$x_2[i] = R \cdot \cos(\text{ang}_1) \cdot \sin(\text{ang}_2).$$

$$x_3[i] = R \cdot \cos(\text{ang}_1) \cdot \cos(\text{ang}_2) \cdot \sin(\text{ang}_3).$$

.

.

.

.

.

$$X_n[i] = R \cdot \cos(\text{ang}_1) \cdot \cos(\text{ang}_2) \cdot \dots \cdot \cos(\text{ang}_{n-1}) \cdot \cos(\text{ang}_n).$$

31. A method as claimed in claim 30, wherein said multi-bit text size is given by  $n \cdot i$ .

32. A method as claimed in any one of claims 27 - 29, wherein a second encoding factor is applied to said multi-bit text of said first encoding factor; said second encoding factor comprising the application of a HASH algorithm.
33. A method as claimed in claim 27, wherein said transactions are online electronic funds transaction between a user, at least one seller and a bank.
34. A method as claimed in claim 27 wherein said multi-bit text is less than or equal to a 1000 bits and said multi-dimensional sphere is less than or equal to 50 dimensions.
35. A method as claimed in claim 27, wherein said system further includes an additional password-based user-identification including an alphanumeric string to confirm the identity of a user by the code engine of the system.
36. A method as claimed in claim 35, wherein said key is initially randomly generated by said code engine upon a request from the client following verification of said password-based user identification and then supplied to said client via a secure network connection.
37. A method as claimed in claim 36, wherein a subsequent key is generated by said code engine after successful authentication of a client following application the clients password and existing key, whereupon a new key is generated and supplied to the client.
38. A method as claimed in claim 29, wherein said portable medium is selected from, but not limited to the group: CD-R, CD-RW or DVD-RW media, USB keys, flash cards, floppy discs, smart chip/card.
39. A method as claimed in claim 38, wherein said portable medium is included in a

multi-media multipurpose business card.

40. A method as claimed in claim 38, wherein said portable medium is incorporated into a mobile phone.
41. A method as claimed in claim 38, wherein said portable medium is incorporated into a smart card.
42. A method as claimed in any one of claims 39-41, further incorporating a short-range bi-directional RF transmitter.
43. A method as claimed in claim 42, wherein said transmitter is a RFID unit.
44. A method as claimed in claim 32, further utilising public key encryption of data exchanged between the user and said security system, wherein said public key encryption includes a public key comprised of said security key parameters uniquely generated for public usage by the security system and one or more client users, and private security key parameters.
45. A method as claimed in claim 44 (when dependant on claim 29), providing dynamic authentication wherein for each user transaction session,
  - said security system generates a dynamic public security key and transmits same to the client after encryption using said public key;
  - the client decrypts said dynamic public security key using the public key sent from the security system;
  - the security server generates a transaction session random number corresponding to said security key parameters and transmits same to the client after encryption using said dynamic public security key;

- said client decrypts said transaction session random number using the dynamic public security key and incorporates same into said first encoding factor of the security key to produce a transaction session multi-bit text;
- said second encoding factor is applied to the session multi-bit text and the resultant is encrypted before being sent to said security server;
- the security server decrypts the received data before determining validation of said authentication by comparing with a security key generated from the application of said first and second encoding factors to said private security key parameters stored in said security system.

46. A method as claimed in claim 44 (when dependant on claims 27 or 28), providing dynamic authentication wherein for each user transaction session;

- said security system generates a dynamic public security key and transmits same to the client after encryption using said public key;
- the client decrypts said dynamic public security key using the public key sent from the security system and generates a multi-bit text from the client's existing stored private security key parameters by applying said first and second encoding factors before encrypting the resultant data and sending to the security system;
- the security server decrypts the data using the dynamic public security key and compares with the result of applying the first and second encoding factors to the private security key parameters stored in the security system to verify successful authentication;

47. A method as claimed in claim 46, wherein if said verification is successful, the next dynamic security key parameter is stored on the security server, while the client application also increments the dynamic security key to store the parameters of the next point.
48. A method of confirming the unique identity of a user in an internet transaction, said transaction including electronic funds transfer and confirmation of transactions over the internet, said users including at least one client, at least one recipient and at least one bank; wherein each user communicates with another via the internet and wherein each transaction incorporates the use of a unique security key, characterised in that the method includes:
- providing a security system incorporating computer processor and memory means on which is operated a code engine generating said codes;
  - on application by a client, providing said key comprising: code generated independently from said client and recipient by a code engine, said code including at least two encoding factors,
  - said key being regenerated and supplied to said user for storage in a portable recordable medium upon each successive and successful transaction application by the client whereby
  - a client provides the code to said at least one recipient and said at least one bank upon request for verification for effecting completion of a transaction; and
  - said at least one recipient and said at least one bank electronically confirm veracity of said code with said engine before a transaction occurs.