(12) UK Patent Application (19) GB (11) 2488310 (13) A

(43) Date of A Publication 29.08.2012

(21) Application No: 1101803.3

(22) Date of Filing: 02.02.2011

(71) Applicant(s):
WINFRASOFT CORPORATION
(Incorporated in the Seychelles)
Sound and Vision House, Suite No. 22, Victoria, Mahe, Seychelles

(72) Inventor(s):
Catalin Saga

(74) Agent and/or Address for Service:
Winfrasoft Limited
Atrium Court, The Ring, BRACKNELL, Berkshire, RG12 1BW, United Kingdom

(51) INT CL:
G06F 21/00 (2006.01) ***H04L 9/32*** (2006.01)
H04L 29/06 (2006.01)

(56) Documents Cited:
EP 1868125 A1 **WO 2007/098569 A1**
WO 2007/063346 A1 **US 6246769 B1**
US 20110010763 A1 **US 20090013402 A1**
US 20070226784 A1

(58) Field of Search:
INT CL **G06F, H04L**
Other: **ONLINE: EPODOC, WPI**

(54) Title of the Invention: **A method and system for authenticating a user of a computerised system**
Abstract Title: **A method and system for authenticating a computer user by using an array of elements**

(57) A method for authenticating a user of a computerised system comprises computing an array or grid 100 of elements 102, presenting the array to the user, receiving user input comprising elements corresponding to pre-determined positions 104, 106 within the array, comparing the user input against a known value and authenticating a user if there is a match. The number of unique elements in the array is less than the total number of elements (so that at least one element is repeated). The user input will form a one-time password (OTP), and the pre-determined position (defined by a memorable identification pattern) is not received by the authentication device. A static PIN or password may also be input by a user. The elements may be numbers (digits), letters, symbols, other characters, shapes or colours. The number of unique elements may be greater than four; each element may be represented at least twice and distributed substantially evenly amongst the array.

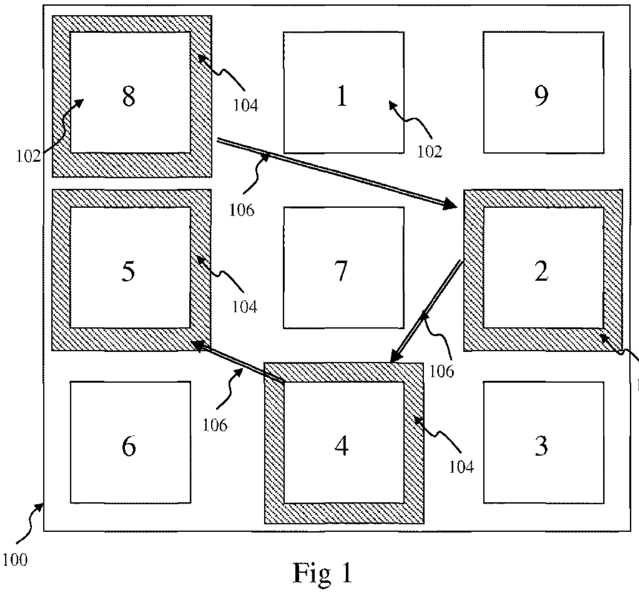

Fig 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

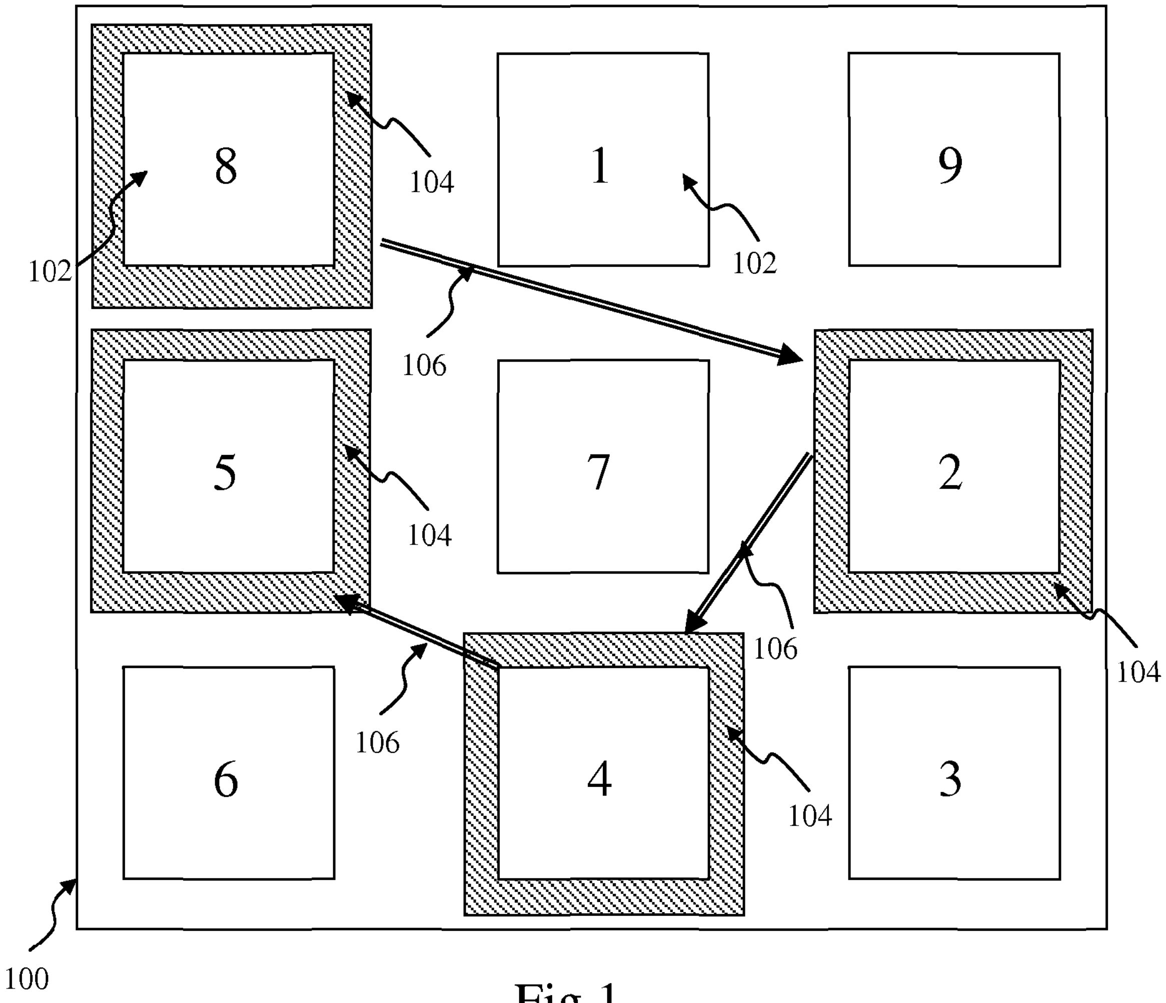

Fig 1

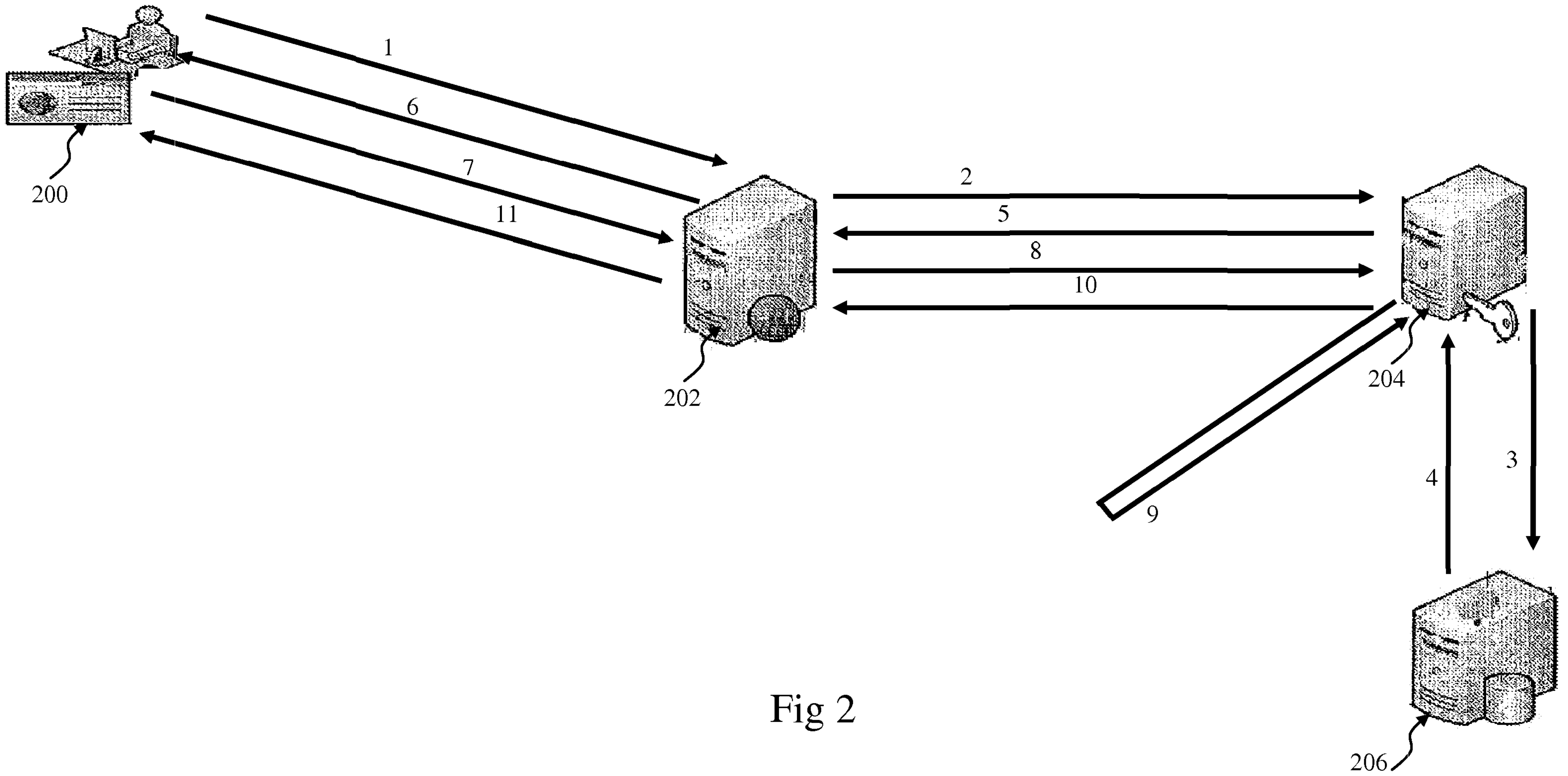

Fig 2

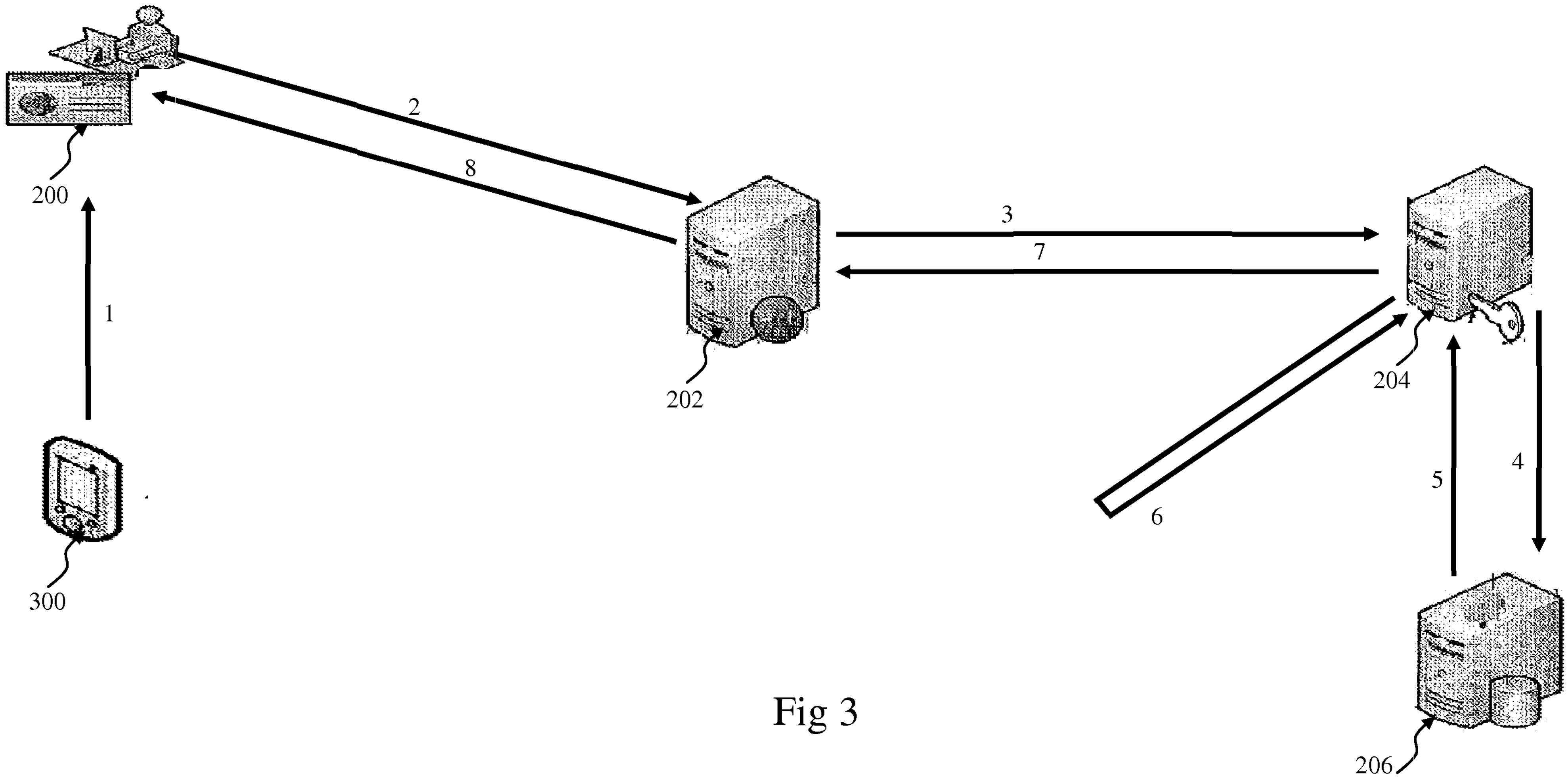

Fig 3

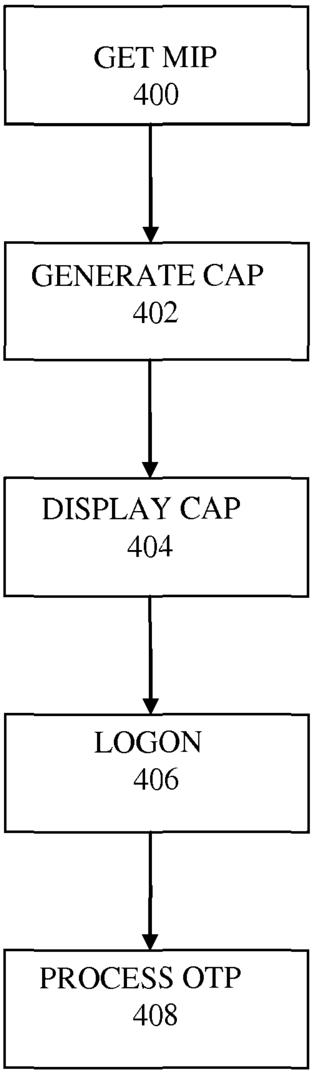
GET MIP
400
GENERATE CAP
402
DISPLAY CAP
404
LOGON
406
PROCESS OTP
408

Fig 4

02 03 11

Passcode Validation Data Flow Diagram

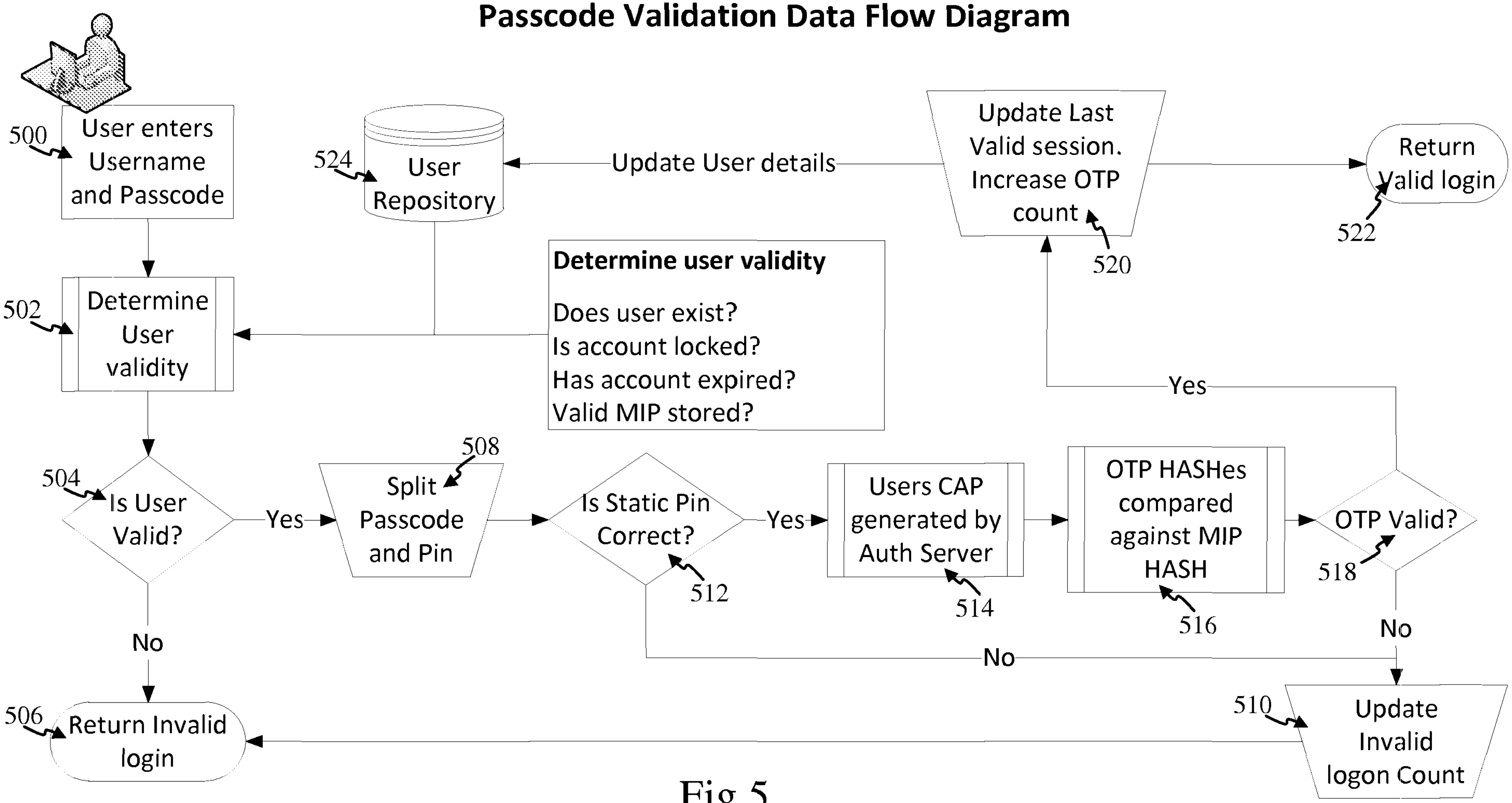

Fig 5

A METHOD AND SYSTEM FOR AUTHENTICATING A USER OF A COMPUTERISED SYSTEM

The invention relates to a method and system for authenticating a user of a computerised system.

One known authentication approach involves the user entering a personal identification number (PIN) via a keypad. More recently, alternative approaches have been developed which involve the use of a memorable identification pattern (MIP). In this case the user inputs a sequence of symbols in the form of a one time pin (OTP) which is derived by overlaying memorable sequence positions against a larger series of elements presented on a display with the addition of an optional static PIN.

Referring to Fig. 1, a display generally designated 100 shows a series of nine elements 102 displaying randomly generated indicia such as digits. The user enters digits according to the MIP for example the shaded elements 104 in the order shown by the arrows 106. Hence even if the numbers change in a subsequent rendering, with knowledge of the numbers then displayed in a given rendering and the sequence of entries by a user corresponding to the MIP, authentication can be achieved.

For example in US patent no. 6246769, a series of numbers are generated in a matrix or grid and the user selects the relevant numbers according to a secret pattern assigned to that user. This can be compared with the expected values to authenticate the user. WO2007/063346 and US6141751 similarly rely on various types of pattern overlaid on a matrix or grid of numbers. GB2366966 allows comparison of a user’s mask code with a linear array of characters.

Various problems arise with the known solutions. For example in some instances random generation of numbers within the matrix, grid or linear array can give rise to inherently unsecure systems. In systems where the grid or matrix is remotely generated, systems can require information about the entire grid or parts of it to be transmitted along with the user entered values which again can provide security risks. In other instances again, remote generation of the grid is not possible.

Embodiments of the invention are set out in the claims. Because the number of unique elements identified is a function of the number of the elements in the array, the level of security is enhanced.

Embodiments of the invention will now be described, by way of example, with reference to the drawings of which:
Fig. 1; shows a conventional grid pattern;
Fig. 2; shows architecture for applying in-band authentications;
Fig. 3; shows architecture for applying out-of-band authentication;
Fig.4; is a flow diagram showing an authentication process; and
Fig. 5; is a flow diagram showing data flow for passcode validation.

For purposes of simplicity various definitions are provided below merely for clarity. They do not affect the scope of the invention, which is defined in the claims, in any way.

PIN - Personal Identification Number
OTP - One Time PIN
Passcode - The code entered by a user consisting of an OTP and optional static PIN
MIP - Memorable Identification Pattern

CAP - Challenge Authentication Prompt

Authentication Device – A physical device, either electronic or analogue, which is able to generate a CAP.

Authentication Authority – An electronic device, typically a computer running specific software, which can process Passcode information and either grant or deny access accordingly, store PIN and hashed MIP information and act as an Authentication Device.

In overview the approaches described herein provide a system in which a user is securely authenticated by inputting a Passcode made up of a sequence of elements in the form of a One Time PIN (OTP), derived by overlaying memorable sequence positions against a larger series of pseudo-random elements presented in an array of elements generated by an Authentication Device together with an optional static PIN/password.

The user both memorises and registers a Memorable Identification Pattern (MIP) with the authentication authority, or the user memorises a MIP that was generated on behalf of the user either automatically or manually. Each time a user needs to prove their identity to the Authentication Authority they are presented with a Challenge Authentication Prompt (CAP) – that is an array or sequence of elements against which the MIP can be overlaid generated by an Authentication Device. The user will derive their OTP by identifying the elements on the CAP that match the positions of their MIP, hence inputting a subset of the displayed elements corresponding to respective pre-determined positions within the array.

The key to the security of the system is that even if the OTP is intercepted in transit along with the CAP then the MIP still remains unknown. If the CAP is provided to the user via a separate physical medium to that used to enter the

OTP ("out-of-band" rather than "in-band") then the security of the system is strengthened further.

As an additional option, the user could also be required to memorise and register a PIN/password with the authentication authority, or the user memorises a PIN/password that was generated on behalf of the user either automatically or manually, or the system can leverage an existing PIN/password already known to the user. When entering a Passcode, a user would need to supply both their OTP code and their PIN/password, in any order. Doing so further protects the MIP from being discovered. Furthermore the number of possible combinations for a correct login increases exponentially as the Passcode length is now the length of the OTP code and static PIN/password combined.

Embodiments include an in-band mode and an out-of-band mode. In the in-band mode the authentication authority which permits access based on the authentication routine is the authentication device, the CAP and passcode may be transmitted by the same medium, the CAP is generated by a seed which is generic or unique to the user and, as explained in more detail below, iterations of the CAP window (that is, a sequence of different CAPs generated across time) do not need to be taken into consideration during authentication.

In the out-of-band mode, the authentication authority processing passcode information is not the authentication device which generates the CAP as seen by the user. If the authentication device is not the same device that is displaying the CAP then the CAP and passcode should not be transmitted via the same medium, as this can allow interception and, over repeated interceptions, possible decoding of the MIP. Instead unique information about the authentication device is registered with the authentication authority for use by a specific user, such as hardware ID, MAC address, IMEI number, Roll/Account number and so forth and this information can be used during the seed generation process for obtaining the CAP. Additionally user specific information may be registered with the authentication device for use during seed generation. The same information can be used for generating the CAP at the authentication device and authentication authority allowing remote generation and comparison and iterations of the CAP window will be taken into consideration during authentication to cater for time synchronisation differences between the authentication authority and the authentication device.

In-band is a term to infer that the authentication is stronger than traditional username+password methods, but is not as strong as true out-of-band. In reality, in-band is single factor (something you know – the MIP) but it is made more secure because the thing that is known is never divulged, unlike a password.

In an out-of-band scenario there is something you have and something you know, in this case a CAP and a MIP. A CAP can be something you have when it is generated/presented on a device using a seed that is unique to that device. As such, without actual possession of the device the CAP would not be known thus a successful logon would not be possible even if the user had knowledge of the MIP. Even in an out-of-band scenario the "something you know" is never divulged thus it could be argued that the system is more secure than traditional two factor authentication methods.

When a CAP is generated using a generic or seed specific to the user it would be considered to be in-band. The transmission method for the CAP and Passcode would typically be the same, i.e. in-band, e.g. logging on to a system via a web page where the CAP is displayed on the page and the Passcode is entered on the same web page.

When a CAP is generated based on unique object specific seed data it would be considered to be out-of-band. The CAP would typically be generated directly on the device displaying the CAP, hence the CAP is never transmitted. However, if a CAP is generated on an Authentication Device separate to which it is displayed, the mechanism used to transmit the CAP must be physically separate to the transmission method used for the resulting Passcode, i.e. out-of-band. This is required to ensure that the CAP and Passcode cannot be simultaneously intercepted, for example in an application running on a mobile phone which uses the devices serial number as a component of seed used to generate and display the CAP. Alternatively a central server could generate a CAP using a mobile phone number as a component of the seed used to generate the CAP, then transmit the CAP to the mobile phone via SMS/TEXT/Picture message. The user then enters their Passcode onto a web page or reads it to a telephone operator for verification.

In one embodiment involving authenticating to a website, for example for Internet Banking, the process would involve a financial institution randomly generating a MIP for a user and securely sending it to them along with basic login instructions, for example physically via the postal service. The user may be supplied with a separate PIN, or may be instructed to use the PIN they already use for their ATM card.

The user would then load the Internet Banking web page and enter their username or ID. A CAP would be displayed on the web page (in a format chosen by the bank) from which the user would need to derive their OTP code using their MIP. The user would then enter a Passcode made up of the OTP code and, if required, an additional PIN.

If the OTP and PIN can be successfully validated then the user is granted entry, otherwise access is denied.

This in-band process is very simple for a user to follow and very low cost for a bank to implement. It also provides a much higher level of security than that of a static username and password without the overhead of a full out-of-band solution which may be ideal for consumer customers. Being able to leverage existing user PIN's and postal distribution methods also provides obvious advantages.

In an embodiment involving authentication to a computer network, remote access is gained via a VPN solution where a user must enter a username and Passcode to gain entry.

The organisation would typically auto generate MIP's for the users and have them emailed directly to the users. For privileged accounts a manual MIP registration process may be required.

The users will be configured to use a separate entity such as their existing mobile phones as a physical token. Where possible a phone application will be installed on the phone and the CAP generated locally. Unique information about the phone hardware would be registered against the user. If a user's phone is not capable of running an application the phone number could be registered against the user and the CAP will be sent to the phone via SMS/TEXT messaging.

When establishing a VPN connection, the user would load the VPN client application on the PC or host computer and enter their username and Passcode. Their Passcode is derived by using the MIP displayed on their mobile phone via the application or SMS/TEXT message, together with an optional PIN/password.

This out-of-band solution is highly secure and leverages many existing components such as phones, VPN gateways and directory services. A new optional PIN can be registered or the user may use their existing network password to lower the burden of having to remember additional information.

Turning to embodiments of the invention in more detail, the in-band and out-of-band computer architectures suitable for implementing the invention can be understood with reference to Figs 2 and 3 respectively.

Turning firstly to Fig. 2 a user 200 at a PC, hosts computers or other access device, interacts via a web server 202 with an authentication server 204. The authentication server 204 may further interact with a user repository server 206 storing user information for use by the authentication server. The entities then interact in a sequential set of steps numbered in the Figure as follows:

1. User attaches to website and inserts user name at workstation 200;
2. Web server 202 sends request to authentication server 204;
3. Authentication server 204 requests user specific information from repository server 206;
4. Repository server 206 sends user information to authentication server 204;
5. Authentication server 204 generates CAP and sends to web server 202;
6. Web server 202 presents CAP to user;
7. User enters one time passcode based on their known MIP;
8. Web server 202 presents OTP to authentication server 204;

9. Authentication server 204 validates and analyses OTP. These steps are set out in more detail below, but in overview, the user validity is determined, the user's CAP is generated or replicated in memory for example by replicating the generation algorithm known to have occurred at the authentication server authentication device (i.e. step 5). The OTP may be part of a passcode including a static PIN which must be extracted as discussed below, and may be stored reversibly or non-reversibly. In the latter case, again as discussed in more detail below, a hash (that is a one way function performed on the OTP) is compared to the stored MIP hash and if there is a match then OTP validity true is returned. If the hashes do not match then OTP validity false is returned;

10. The authentication server 204 returns the authentication validity to the web server 202;

11. The web server 202 presents the authentication validity to the user at workstation 200 allowing system access to take place.

Referring to the out-of-band authentication process shown in Fig. 3, in addition to the hardware displayed in Fig. 2 a token or other external device such as a mobile telephone 300 is shown. The steps performed comprise:

1. The external device 300 generates the CAP and viewed by the user;

2. The user attaches to the website at the workstation 200 and inserts user name and one time passcode;

3. The web server passes the request to the authentication server 204;

4. The authentication server 204 requests user specific information from the user repository server 206;

5. The user repository server 206 sends the user information to the authentication server 204;

6. The authentication server 204 validates and analyses the one time passcode optionally including a static PIN. User validity is determined, the user's CAP is generated in memory, and again as discussed in more detail below, the hash

of the OTP is compared with the stored MIP hash running the generation algorithm for a series of possible time "windows" and true/false validity returned as appropriate;

7. The authentication server returns the authentication validity to the web server 202;

8. The web server 202 presents the authentication validity to the user to allow subsequent access to the system.

It will be appreciated that the individual hardware elements can be any form of appropriate processor or interface device and that communications can be over any appropriate system or network such as the Internet, a local intranet and so forth. Processes can be embedded in instructions stored in a computer readable medium and implemented in any appropriate manner including software, firmware and hardware. Any appropriate generating algorithm can be adopted for generating the CAP, and any appropriate hashing algorithm can be adopted for creating a hash for comparison, as will be well known to the skilled reader.

Turning to operation of the process in more detail, Fig. 4 shows the principal steps involved. In overview at step 400 the MIP is obtained, at step 402 the system generates the CAP, at step 404 the system displays the CAP, and at step 406 the user logs on. The OTP is then processed at step 408 including input of the OTP together with any optional PIN, and validation as discussed in more detail below.

At step 400, therefore, the MIP is generated. This can be achieved in various ways. For example the organisation can auto generate MIPs for users, and e-mail or otherwise communicate them directly to the users. For high security, privileged or specific accounts a manual MIP registration process may be required.

The particular manner in which the MIP is created can be manually by an administrator of the system or automatically generated for example by an authentication authority. In a preferred embodiment the MIP should be encrypted in transit between the entry device and the Authentication Authority prior to it being stored as a HASH. This is critical to ensure the secrecy of the MIP. The encryption strength should be at least 128bit and should use a well-known secure cryptographic algorithm.

When a MIP is manually generated:

1. A method of identifying and selecting the required pattern positions and sequence should be implemented.
2. The user may be present during the MIP creation and may enter the MIP directly into the system without the administrator having knowledge of the MIP.
3. The MIP should be communicated to the user in a secure manner, typically in accordance with an organisational security policy. The delivery mechanism may be, but is not limited to, electronic mail, text/sms message, instant messaging systems, paper protected by some physical security and trusted delivery mechanism.
4. A method allowing the user to change the MIP should be implemented.
5. The user may be forced to change their MIP after first use or at set intervals.
6. The user should be able to change their MIP after first use.

When a MIP is automatically generated:

1. The MIP should be communicated to the user in a secure manner, typically in accordance with an organisational security policy. The delivery mechanism may be, but is not limited to, electronic mail, text/sms message, instant messaging systems, paper protected by some physical security and trusted delivery mechanism.

2. A method allowing the user to change the MIP should be implemented.
3. The user should be forced to change their MIP after first use.
4. The user should be able to change their MIP after first use.

Further security steps can optionally be implemented in relation to the MIP. In one embodiment various steps can ensure that they MIP remains fresh and complex, as follows.

- A MIP should have a minimum age configuration option which should be set to 2 days.
- A MIP should have a maximum age configuration option which should be set to 42 days or less and should be greater than the minimum age, but should be allowed to never expire.
- A record of previous used MIP's should be kept to ensure that a previously used MIP is not re-used. The number of historical retained MIP's should be a configurable option and should be set to at least 24.
- The number of elements in a MIP (aka the MIP length) should be a configurable option, should be set to a minimum of 6.

Restricting the use of common MIP patterns should be a configurable option.

In an embodiment of the system a user account is locked out after a configured number of bad logon attempts. This is required to reduce the risk of a brute force attack. The account lockout period should be configurable and should not require manual intervention for unlocking.

The CAP is generated at step 402 according to a process, in a preferred embodiment, ensuring that a balance is struck between CAP length and number of unique elements allowing high levels of security.

A MIP and a CAP have many interdependencies and their usage requires strict control to maintain the security of the system. For example, a CAP consisting of twenty letter "A"s would provide little to no security. As such strict controls must be enforced by the system to maintain the high levels of security it offers:

1. The MIP should not be stored in such a way that is could ever be recovered or reassembled. This should be achieved by using a Federal Information Processing Standards (FIPS) compliant secure HASH function as per FIPS 180-3 (http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf).
2. If a MIP is lost or forgotten then it should be re-created as it cannot be recovered.
3. The CAP should be generated using a Federal Information Processing Standards (FIPS) compliant keyed-hash message authentication code (HMAC) e.g. FIPS 198 (http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf). Alternatively, derivatives of RFC 4226 "HOTP: An HMAC-Based One-Time Password Algorithm" (http://tools.ietf.org/html/rfc4226) or RFC 2289 "A One-Time Password System" (http://tools.ietf.org/html/rfc2289) may be used.
4. The MIP should not be transmitted during the authentication process and should be kept secret at all times.
5. The greater the total number of element positions a MIP has (MIP length) the more secure it is. A MIP made of up of one or two element positions could be cracked fairly easily. As such the MIP length should be reasonably long; generally its length should be akin to that of a long PIN or a short password. Ideally a MIP should consist of at least 6 element positions to balance security with usability.
6. The greater the total number of elements a CAP has (CAP length) the more secure it is. A larger CAP length number also allows for a greater quantity of unique elements which, when combined with the MIP length

results in many more possible combinations for an OTP. The CAP length must also be balanced with the CAP display requirements and what method will be used to assist a user with locating their memorable positions in the CAP. The CAP should not be too short otherwise the OTP could be cracked fairly easily. When determining the CAP length, the CAP display format and usability factors should be taken into consideration along with security. A reasonable balance would typically result in a CAP length of approximately 30 elements, and preferably not fewer than 10 elements.

7. One of the key aims of the system is to keep the MIP a secret. To do so it should not be possible to determine the MIP when given the CAP and a valid OTP code for example by observation or interception. If every element on the CAP was unique then it would be very simple to determine the MIP as every position is uniquely represented. Conversely, if only a single element was represented multiple times on a CAP then the OTP would be very simple to determine as it would always be the same. As such, either extreme has severe security flaws and should not be used. A balance must be struck between having enough repetitions of each element to protect the MIP, and enough unique elements to protect the OTP. Preferably the number of unique elements in the CAP should be greater or equal to 4 and should not be greater than one above the greatest integer square root of the total number of elements in the CAP, which value is found to allow an ideal balance to be struck for overall security. For example, if there are 20 elements then each should be able to take one of at least 5 [=INT(√20)+1] unique values, giving an average unique element repetition rate of 4 [=20/5].

8. The order of elements displayed in the CAP is not important from a security perspective, but it is important to ensure that there is an even

spread of each element used. A scenario where a CAP has 5 unique elements and is 25 elements in length may seem to strike the right balance of usability and security. But if elements 1 through 4 are only listed once, and element 5 is listed 21 times then the security is again seriously flawed, although not to the same extreme as discussed previously. To avoid this scenario each unique element must be present the same number of times in a CAP; as far as is mathematically possible given the CAP length. So for example, each unique element in the CAP should be repeated at least 1 less than the greatest integer square root of the total number of elements in the CAP, and should not be repeated more than the greatest integer square root of the total number of elements in the CAP. This is required to enforce even element repetition across various CAP lengths.

In terms of the actual generation of the CAP, a CAP is generated by an Authentication Device typically each time a user wishes to logon, but could be generated prior to the logon event. The CAP may be displayed on the actual Authentication Device or on a separate device that the user has access to. For example, CAP may be rendered by a central server and remotely displayed to a user via a web browser on a PC, or sent to a mobile phone via TEXT/SMS, or printed on a piece of paper. Alternatively the Authentication Device could be an application running on a mobile phone where it is both rendered and displayed.

As discussed above, each CAP is designed to be unique as much as mathematically possible based on the constraints of the crypto algorithm used and the number of elements in the CAP. A key part of generating a CAP is the date and time, as the same device should generate unique CAPs at different time intervals. For an electronic token this may be every minute, but for a paper based system this may be every month.

Each CAP should have a CAP Window which is a period of time that the CAP is valid for. This is required to allow the user ample time for the OTP to be entered before the CAP expires. The time period for the CAP Window should be configurable. The CAP Window begins when the CAP is generated. An OTP provide by the user based on the CAP should be presented within the CAP Window, or configured iterations of the CAP Window, for the authentication to be successful.

As discussed above, a CAP is generated using various pieces of unique information which make up a "Message" and a "Seed". The result produces a pseudo-random dataset which must be interpreted to match the requirements and constraints of the system implementation.

The Message is constructed using the current UTC date and time, and an Identifier.

- The date and time is constructed based on ISO 8601 (http://www.w3.org/TR/NOTE-datetime) format as follows: YYYYMMDDhhmm. ISO 8601 dictates that the hour value is based on a 24hour clock.
- The Identifier is a number which should change every time a new CAP is generated within the same CAP Window following a logon attempt. The change may be incremental or random but should not be repeated during the same CAP Window. Once the current CAP Window has elapsed the counter is reset. The Message length should be at least 13 characters, the first 12 always contain the date and time information and the remaining characters contain the counter information. The identifier

is key to ensure that the Passcode is a true One Time Pin and cannot be reused during the same CAP Window otherwise the system would be susceptible to a credential replay attack.

Message example: 2010021409553

The Seed is a unique identifier (GUID/UUID) which is unique to a user or Authentication Device which should conform to RFC 4122 "A Universally Unique IDentifier (UUID) URN Namespace" (http://tools.ietf.org/html/rfc4122). The seed MAY be constructed based on device or hardware specific information.
Seed example: 489ea326-af2e-4bed-bf09-695ee66a4d66

The Message and the Seed should be run through a HMAC routine to produce a pseudo-random dataset. The resulting dataset should be interpreted/abstracted via a set formula which takes into account the chosen symbol format, the total number of elements, the number of unique elements and the symbol repetition restrictions to produce a CAP.

Once the CAP is generated it is displayed at step 404. There are no restrictions on how a CAP is displayed to a user other than there should be a method employed for the user to understand and identify the elements in the CAP.

1. The CAP should be a simple string of text based alphanumeric characters, pictures or themed elements. It can be displayed horizontally, vertically, or line wrapped.
2. Visual aids to help the user identify positions in the CAP should be used. This may include the creative use of symbols, shapes, colours, layouts, backgrounds, fonts, sounds and textures.

3. The display of the CAP should be as appropriate as possible to the display capabilities of the Authentication Device.
4. The CAP may be based on audible prompts or sounds which can be recognised as "audio elements" for the visually impaired. A tactile CAP may be used based on shapes, textures or brail.

For example, a CAP could be

- a straight line of numbers with alternating font colour every 5 characters;
- overlaid onto a Chess board / Sudoku square or a 3 dimensional cube;
- a line wrapped row of letters every 4 characters.

At step 406, the Passcode logon request by a user at a workstation is processed. An Authentication Authority must be able to validate a Passcode value given to it and determine if it is valid or not. When a user logs on to a system they should provide a username/ID to identify themselves. In addition they should provide a Passcode for authentication which should include an OTP code and may also include a static PIN/password.

The Authentication Authority should first check if the user is required to use a static PIN/password along with an OTP by checking the user account properties in a database. This initial step is key to determine the processing path.

If a PIN/password is required the Authentication Authority should attempt to separate the PIN and the OTP from the Passcode so that the OTP can be processed separately, but only if the PIN/password is valid.

If the PIN/password is stored in a reversible manner, it may be entered anywhere in relation to the OTP. Because the PIN/password should be contiguous, a test can be performed whereby the securely stored PIN/password is decrypted and sought within the Passcode. If a match is found the actual PIN/password is known and it can be removed from the entered Passcode to reveal the remaining OTP characters. If a match is not found then the authentication will instantly fail and no OTP processing shall occur.

If the PIN/password is not stored in a reversible manner, e.g. only a hash is stored, then the PIN/password must entered either before or after the OTP code. In addition, either the length of the OTP or the PIN/password should be known so that the Passcode can be split into OTP and PIN/password components. Once split, the PIN/password can be verified in a manner appropriate to the storage mechanism, e.g. comparing the hashes of the PIN/password. If the PIN/password can be verified then the OTP processing can occur.

There is a statistical chance that the OTP sequence could match or contain a subset of the static PIN. This scenario should be explicitly catered for otherwise the incorrect OTP characters may be tested and authentication would fail. To prevent this situation from occurring, when a valid PIN hash match is found the sequence used for the PIN should be tested against the remaining Passcode sequence and if a further match is found then each possible OTP code must be determined for further processing.

When the OTP code is augmented with an additional static Personal Identification Number (PIN) or password; a preferred set of requirements is set out below. The user both memorises and registers a PIN/password with the Authentication Authority, or the user memorises a PIN/password that was generated on behalf of the user either automatically or manually, or the system can leverage an existing PIN/password already known to the user. When the user enters their OTP during an authentication process they should also enter their static PIN/password at the same time.

1. The PIN/password can be entered before, in the middle of, or after the OTP code. The Authentication Authority will decipher the information entered to separate the OTP from the PIN.
2. A configurable policy should be made available to allow the position of the PIN in relation to the OTP to be fixed to a required orientation. An embodiment may need to force the position of the PIN/password in relation to the OTP for scenarios where the PIN/password is not stored in a reversible format and the length is unknown.
3. The elements used for the PIN should be a subset of the elements used within the CAP in in-band factor scenarios. This is required to maintain the secrecy of the PIN characters vs. the OTP characters. In out-of-band scenarios this is not required as the Passcode and CAP are not available at the same place at the same time.
4. There are not many methods available which can be used to secure a PIN/password, however length is a key factor. Users typically find it difficult to memorise lengthy PIN numbers and complex passwords, as such a balance must be found between usability and security. Users should typically be comfortable with 4 digit PINs as they are used by most bank ATM cards, as such 4 or more is an ideal number.

For example: if a user registers a MIP based on the following sequence positions: 1st, 15th, 7th and 9th. Additionally, the user registers a PIN of “9999”. If the user is presented with the CAP “0 8 0 6 1 8 7 9 6 7 0 9 0 1 8 7 6 6 8 7” then the OTP would be “0876”. As such the user MAY enter 99990876, 08769999 or 08999976, or any combination so long as the PIN remains contiguous.

Once the OTP is entered it is processed at step 408. To process the OTP code(s), the Authentication Authority should perform the same operation as an Authentication Device to recreate the same CAP used by the user when they entered the Passcode. The Authentication Authority now has access to both the CAP and the OTP, but does not have direct access to the MIP as only a hash of the MIP is stored. Since each symbol on the CAP is repeated multiple times the Authentication Authority must iterate every possible MIP hash value based on the CAP and OTP and compare it with the hash value stored in the database. If a match is found then the authentication is successful, if not then the authentication fails. Although this process may result in thousands of mathematical operations per authentication request the process the complexity of the mathematical operations is considered extremely low demand for any modern CPU.

If the Authentication Authority is processing an out-of-band request then the tests must be run against multiple CAP's based on iterations of the CAP Window. If "n" is now in time, the iteration testing should increment as follows: n+1, n-1, n+2, n-2, n+3, n-3 etc. This logic assumes the clocks of the Authentication Authority and the Authentication Device are more closely synchronised and should produce a positive answer with less CPU overhead. An authentication device may memorise the correct iteration offset value and use that value for n as a default offset for subsequent authentication requests. This may help to improve authentication performance and lower CPU load on the Authentication Authority.

The approach can be further understood with reference to Fig. 5. At step 500 the user enters their user name and Passcode and the user validity process is commenced at step 502. If at step 504 the user is not valid then an invalid login is returned at step 506. Otherwise at step 508 the OTP and PIN are separated as indicated above.

At step 512 the static pin is checked. If it is not correct then an invalid log on count is incremented at step 510 and an invalid log on is returned at step 506. Otherwise the user's CAP is generated by the authentication server at step 514 and the hash comparison described above is performed at the authentication server at step 516. If at step 518 the OTP is not valid then at step 510, once again the invalid log on count is updated at step 510 and an invalid log on is returned at step 506.

Otherwise, at step 520 the last validation session is updated and the OTP count is augmented. A valid log in is returned at step 522, user details are updated if appropriate at step 524 and the process returned determining user validity for next session entry.

Implementation of further embodiments can be understood with reference to the discussion above. For example in one implementation authentication takes place over the telephone using a paper based token for example where a customer calls a utility company customer service line.

A typical embodiment of this scenario would involve a customer of a utility company needing to authenticate themselves to the utility company over the phone to request changes to his/her account information.

In this case, the utility company may have decided to integrate the system into their accounting and billing system. A random MIP is generated for the customer and securely sent to them along with basic instructions on how it will be used. The most likely method of sending the MIP would be physically via the postal service.

Every time a customer invoice or statement is produced a CAP is generated using unique information on the document for the seed and placed on the document. As such, the invoice or statement is the actual token. When a customer telephones the customer services desk all they need is a statement or invoice to hand. The customer services operator would need to ask for some basic identification information such as the customer name or account number, the document date or document number in order to identify which token is being used, and the customer Passcode. The system is then able to authenticate the user.

An embodiment of this scenario may decide not to enforce the One Time Pin nature of the identifier as if the customer called back within a short period of time they would be required to provide a Passcode from a different document. The security of true OTP must be balanced with usability as in this scenario there are very few iterations of a CAP available.

This approach allows the utility company to negate the requirement to deploy any form of token to save cost, but still benefit from the strength of out-of-band authentication. The customer experience is improved as their identity can be proven with a single question instead of having to divulge a lot of personal information over the phone such as date of birth and their mother's maiden name etc.

In a further embodiment, reverse validation can be achieved over the telephone using a paper based token for example where a utility company customer services operator calls a user. In this scenario the customer needs to ensure that it is the actual utility company that is calling them and it is not a prank or phishing call.

As the customer services operator does not know the customers MIP (as it cannot be retrieved) the reverse of the previous example cannot be performed. However, the customer can be reasonably confident that only the utility company would know what the CAP on a particular invoice or statement was as the customer would have the original copy. A prank or phishing caller is not likely to have a copy of an actual statement or invoice.

The customer can tell the operator which statement or invoice number they are in possession of and the operator is then able to recall that document and read a section of the CAP, or the entire CAP to the customer. The customer services system may even obscure the CAP so that only a portion of it is shown and confirmed with the customer. The customer can verify the CAP details on their copy of the document.

Once the customer is satisfied that it is the utility company on the phone, the utility company will still need to make sure the customer is the one they intended to call, in which case the previous example continues.

The MIP has been kept secret at all times and the customer did not have to remember anything to validate the utility company. This embodiment allows the CAP, or sections of the CAP, to be used as a shared secret due to the unique nature of a CAP. The utility company now has a highly cost effective method of mutual authentication between its staff and customers.

It will be seen, therefore, that a simple yet highly secure system can be provided with added protection against third party observation or interception ("shoulder surfing") whilst permitting out-of-band operation, without requiring pre-generated MIPs and with improved security in the generation of the unique elements within a MIP or other array.

It will further be appreciated that the approach can be implemented in any appropriate manner, and according to any appropriate algorithm or set of algorithms and the array can be presented in any appropriate form.

Claims

1. A method of authenticating a user of a computerised system comprising:

computing an array of elements;

presenting to a user the array of elements;

receiving user input comprising a subset of the presented elements corresponding to respective pre-determined positions within the array;

presenting the user input for comparison against a known value; and

authenticating the user if the comparison results in a match;

in which each element in the array is computed to adopt one of a range of unique element identities, the number of unique element identities in the range being a function of and less than the number of elements in the array.

2. A method as claimed in claim 1 in which the element comprises one of a number value, a letter, symbol, shape or a colour.

3. A method as claimed in claim 1 or claim 2 in which the number of unique element identities comprises an integer value which is greater than or equal to 4 and is not greater than one above the greatest integer square root of the total number of elements in the array.

4. A method as claimed in any preceding claim in which the number of appearances of each unique element identity is distributed substantially evenly amongst the array elements.

5. A method claimed in claim 4 in which each unique element is represented at least twice, and repeated at least 1 less than the greatest integer square root of the total number of elements the array.

6. A method as claimed in claim 5 in which each unique element is not repeated more than the greatest integer square root of the total number of element in the array.

7. A method as claimed in any preceding claim in which the user input further includes a user passcode value.

8. A method as claimed in claim 7 in which the user passcode value consists of an OTP and a PIN/password.

9. A method as claimed in any preceding claim in which the number of elements in the array is greater than 10, preferably greater than 20, more preferably greater than 30 elements.

10. A method as claimed in any preceding claim further comprising performing a comparison of the user input against a known value stored at the authentication location.

11. A method as claimed in claim 10 in which a set of computed hashes of possible correct patterns based on the user input in response to the array is constructed.

12. A method as claimed in claim 11 in which the comparison is performed by comparing the set of computed hashes against the known hash value.

13. A method as claimed in any preceding claim in which the array of elements is generated and presented to the user, and the user input is received, on a common device.

14. A method as claimed in any of claims 1 to 13 in which the array of elements is generated and presented to the user on a first device and the user input is received on a second device.

15. A method as claimed in any of claims 10 to 14 in which comparison of the user input is performed on the user input device.

16. A method as claimed in any of claims 10 to 14 in which comparison of the user input is performed on a remote device.

17. A method as claimed in claim 16 in which a known value is generated on the remote device by replication of data available to the user.

18. A method of authenticating a user of a computerised system comprising:

receiving data corresponding to a user input based on an array of elements presented to a user;

replicating the elements presented to the user;

performing a comparison of the received user input data and the replicated data, and authenticating the user if there is a comparison match.

19. A method as claimed in claim 18 in which the comparison of the data is based on the result of an extrapolation function which evaluates said data.

20. A method as claimed in claim 18 or 19 in which the replication step is time dependent.

21. A method as claimed any of claims 18 to 20 further comprising identifying and extracting a user PIN/password value from the user input data prior to said comparison step.

22. A computer apparatus programmed to provide authentication of a user of a computerised system, the apparatus being arranged to perform the steps of:

presenting to a user an array of elements;

receiving user input comprising a subset of the presented elements corresponding to respective pre-determined positions within the array;

presenting the user input for comparison against a known value; and

authenticating the user if the comparison results in a match;

in which each element in the array can adopt one of a range of unique element identities, the number of unique element identities in the range being a function of and less than the number of elements in the array.

23. A computer apparatus programmed to provide authentication of a user of a computerised system, the apparatus being arranged to perform the steps of:

receiving data corresponding to a user input based on an array of elements presented to a user;

replicating the elements presented to the user;

performing a comparison of the received user input data and the replicated data, and authenticating the user if there is a comparison match.

24. An apparatus as claimed in claim 23 in which the comparison of the data is based on the result of an extrapolation function which evaluates said data.

25. A computer readable medium comprising instructions arranged to implement the steps of the method of any of claims 1 to 21.

26. A method or apparatus substantially as herein described with reference to the drawings.

Application No:	GB1101803.3	**Examiner:**	Mr Peter Doenhoff
Claims searched:	1-17, 22, 25	**Date of search:**	8 May 2012

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-6, 9-17, 22, 25	WO 2007/063346 A1 (CRAYMER et al.) See figs. 3, 4, 11; p. 11, l. 22 - p. 12, l. 3; p. 19, l. 1 - p. 20, l. 5; p. 21, l. 7-19
X	1, 2, 4-6, 9-17, 22, 25	US 2007/0226784 A1 (UEDA et al.) See figs. 5, 7, 8; paras. 4, 39, 53
X	1, 2, 4-6, 9-17, 22, 25	US 2011/0010763 A1 (BEARDSLEE) See figs. 1-9, paras. 24-27
X	1, 2, 4-6, 9-17	WO 2007/098569 A1 (GOERTZEN) See fig. 2; p. 6, l. 11 - p. 7, l. 5; p. 10, l. 16-31
X	1, 2, 4, 7-17, 22, 25	US 2009/0013402 A1 (PLESMAN) See figs. 3, 4; paras. 19, 20, 34, 57
X	1, 2, 4, 9-17, 22, 25	US 6246769 B1 (KOHUT) See figs. 5A-D; col. 11, l. 53-67; col. 13, l. 18 - col. 14, l. 64
X	1, 2, 4, 9-17, 22, 25	EP 1868125 A1 (SAVERNOVA) See figs. 1-5; paras. 20-28

Categories:

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

Field of Search:

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

Worldwide search of patent documents classified in the following areas of the IPC

G06F; H04L

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

EPODOC, WPI

International Classification:

Subclass	Subgroup	Valid From
G06F	0021/00	01/01/2006
H04L	0009/32	01/01/2006
H04L	0029/06	01/01/2006