

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 September 2006 (28.09.2006)

PCT

(10) International Publication Number
WO 2006/100655 A2

(51) International Patent Classification:

G06F 21/00 (2006.01)

(21) International Application Number:

PCT/IE2006/000015

(22) International Filing Date: 21 March 2006 (21.03.2006)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

S2005/0147

21 March 2005 (21.03.2005) IE

(71) Applicant and

(72) Inventor: MCKENNA, Patrick [IE/IE]; 13 Orchard Close, Coolmine, Dublin 15 (IE).

(74) Agents: LANE, Cathal, Michael et al.; Tomkins & Co., 5 Dartmouth Road, Dublin 6 (IE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,

CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURING ACCESS AUTHORISATION

	a	b	c	d	e	f	g	h	i	j
a	6	21	...							
b										
c										
d				...	362	...			...	7
e										
f										
g										
h										
i					...	7	...			
j					...	94	...			

303
302

102D

	a	b	c	d	e	f	g	h	i	j
a	6	21	...	...	5	...				
b										
c										
d				...	362	...			...	7
e										
f										
g										
h										
i					...	7	...			
j					...	94	...			

303
302

102D

304

102E

(57) Abstract: A system for securing access to an electronic resource is provided, which comprises at least one data processing terminal and a support including at least first and second series of numerical values, said terminal comprising storage means, processing means and display means, said storage means storing a combination of a user reference and an electronic resource user access reference for at least one user and instructions which configure said processing means to generate a third series of random numerical values and request user input in response to said user requesting access to said electronic resource, compare said user input and said electronic resource user access reference upon receiving said user input, and grant access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said first series identified with positioning said support relative to said display device and comparing corresponding numerical value of said second series with corresponding numerical value of said third series.

Title

Securing Access Authorisation

Field of the Invention

- 5 This invention relates to securing access to an electronic data resource stored in a data processing system. More particularly, this invention relates to a device for encrypting one or more user identifiers in reference to numerical series and a corresponding method.

Background to the Invention

- 10 In the so-called information age, an increasing amount of personal and/or user information is disseminated in either isolated or networked data processing terminals, whether as a result of user choice, for instance when registering for online banking services, or as a result of procedural change, such as when government agencies upgrade to computerized systems and records.

15

- The value of this readily-accessible personal or user information is increasing in tandem with the growing ubiquity of highly-distributed networks such as the Internet, as it allows purveyors of goods or services to constantly refine their target markets and extract better revenue from more accurate use of their advertising expenditure. More disturbingly, as the value or nature of this information expands, so it attracts third-party users willing and able to make unauthorized use of all or a portion of this information and therefore the need to implement access authentication methods and systems has long been recognized and many such methods and systems exist in the prior art.

- 20 Password authentication schemes constitute the most widely-used methods of access authentication for a user to access electronic data resources, such as her banking details and/or service provided over the Internet, and this despite growing problems associated with theft of user information, particularly information with an inherent financial value such as credit card or user or bank account details. Indeed, password authentication schemes can be compromised in numerous ways.

- 25 *Trojan Horse Attacks* and *Spyware* are the most classic and widespread types of attack. A Trojan Horse is an application that is stealthily processed by a data processing system and assists in the performance of illicit transactions, unbeknownst to a user of the data processing system. Trojan Horses may be used either on a standalone terminal sharing multiple
- 30

consecutive users, such as in a public library, but are more commonly used in highly-distributed networks, such as the Internet, by remote unauthorised users and are configured to stealthily load into a data processing system and then collate local data including keys pressed, applications processed, electronic resources accessed over the network as well as
5 capture images of graphical user interfaces, for subsequently broadcasting this information over the network, still unbeknownst to the user, to those remote unauthorised users. In this context, Spyware is a colloquialism encompassing both legitimate and illegitimate forms of Trojan Horse applications, which gather information about a user's terminal and use thereof and relay that information to remote users, such as marketing companies in legitimate cases or
10 unauthorised users in illegitimate circumstances.

Phishing Attacks are mounted by highly-organised unauthorised users and comprise large-scale, carefully planned defrauding operations. Phishing is a method of using deceptive email and internet sites to retrieve authentication data from unsuspecting users. Such operations
15 typically begin with an electronic mail message addressed to a genuine user by an apparently genuine sender, for instance the bank of that user or an Internet transaction website at which said user is registered. The message is configured in wording, appearance and interactive features, such as a pointer to a network address or Uniform Resource Locator, to lead the recipient to an apparently genuine Internet page of this bank or transaction site, which is in
20 fact a false Internet page output by the data processing system of the unauthorized users, at which point the user is requested to input her username and password, which are therefore obtained by the afore-mentioned highly-organised unauthorized users when said user is deceived.

25 *Man-in-the-Middle Attacks* are the hardest attack to carry out, as they need to be performed whilst a victim is connected to the network. Such attacks involve a particularly sophisticated form of data processing procedure, colloquially known as hacking, which involves the illegal misuse of Secure Socket Layer Certificates and Keys.

30 The negative impact of any successful attack is threefold: bad publicity for the provider of the electronic resource, loss of confidence by users as a subsequent reaction and financial loss from the attack itself to the provider and/or the users. Loss of customer confidence may reflect not only on the image and turnover of a provider, but also on the Internet as a channel for transacting with sensitive information. For obvious reasons, institutions are keen to reduce
35 their exposure to these risks. It is unfortunate that this type of unauthorized activity will

become more intense with the ongoing drive to facilitate the transacting of an ever-increasing amount of goods and service over the Internet.

5 An improved system and an improved method are therefore required to prevent unauthorized users from obtaining user information, particularly access authentication data, by deception, whether a user accidentally or unknowingly provides this information or whether such unauthorized users deliberately attempt to obtain this information by deception.

Object of the Invention

10 It is an object of the present invention to improve the security of access authentication required for a user to access an electronic resource, whether locally or via a network, by decreasing the risk of compromising authentication data.

15 It is another object of the present invention to provide a method of securing access to an electronic resource at a user terminal.

It is a further object of the present invention to provide a system for securing access to an electronic resource.

Summary of the Invention

20 According to an aspect of the present invention, a method of securing access to an electronic resource is provided at a user terminal equipped with a display device, which comprises the steps of

25 providing a user with at least first and second series of numerical values on a support;
storing a combination of a user reference and an electronic resource user access reference for said user;

in response to said user requesting access to said electronic resource, generating a third series of random numerical values and requesting user input ;

30 upon receiving said user input, comparing said user input and said electronic resource user access reference; and

granting access to said electronic resource upon said comparison returning a match,
wherein said user input comprises at least one numerical value of said first series identified with positioning said support relative to said display device and comparing corresponding numerical value of said second series with corresponding numerical value of
35 said third series.

According to another aspect of the present invention, a system for securing access to an electronic resource is provided, which comprises at least one data processing terminal and a support including at least first and second series of numerical values, said terminal comprising
5 storage means, processing means and display means, said storage means storing a combination of a user reference and an electronic resource user access reference for at least one user and instructions which configure said processing means to

generate a third series of random numerical values and request user input in response
10 to said user requesting access to said electronic resource;

compare said user input and said electronic resource user access reference upon receiving said user input; and

grant access to said electronic resource upon said comparison returning a match,

wherein said user input comprises at least one numerical value of said first series
15 identified with positioning said support relative to said display device and comparing corresponding numerical value of said second series with corresponding numerical value of said third series.

According to yet another aspect of the present invention, a support is provided for securing
20 access to an electronic resource, said support comprising at least first and second series of numerical values, said support being operationally positioned relative to the display device of a data processing terminal on which a third series of numerical values is displayed in response to a user requesting access to an electronic resource, wherein said user may compare corresponding numerical value of said second series of said support with corresponding
25 numerical value of said third series and input at least one numerical value of said first series identified by said comparison for granting access to said electronic resource upon the comparison of said user input and an electronic resource user access reference returning a match.

30 Preferably, the support comprising said first and second series of numerical values is configured with at least one substantially see-through portion between said series, and the step of comparing corresponding numerical value of said second series with corresponding numerical value of said third series advantageously comprises the further step of positioning the see-through portion of the support over the third series on the display device.

The first, second and third series of numerical values may comprise a number of numerical values, each of which is comprised between 0 (zero) and 9 (nine). In a preferred embodiment, the number of numerical values is ten.

5 The third series is advantageously generated as a random series to uniquely encrypt the electronic resource user access reference for every access authentication procedure. The first, second and third series of numerical values are preferably spaced relative to one another both on the support and the display device, to facilitate the comparison therebetween.

10 In an alternative embodiment of the present invention, the terminal is connected to a network and the electronic resource is a data resource stored at a first remote terminal.

In another alternative embodiment of the present invention, the terminal is connected to a network, the electronic resource is a data resource stored locally or at a first remote terminal
15 and the combination of a user reference and an electronic resource user access reference for said user is stored at a second remote terminal.

In yet another alternative embodiment of the present invention, the terminal is connected to a network, the electronic resource is a data resource stored locally or at a first remote terminal,
20 the combination of a user reference and an electronic resource user access reference for said user is stored locally or at a second remote terminal and the third series is generated at said second remote terminal and communicated to the local user over the network.

In a further aspect of the present invention, a method of securing access to an electronic
25 resource is provided at a user terminal equipped with a display device, the method comprising the steps of:

providing a user with a first series of personal numerical values and with a second series of numerical values on a support;

storing a combination of a user reference and an electronic resource user access
30 reference for said user;

in response to said user requesting access to said electronic resource, generating third and fourth series of random numerical values and requesting user input ;

upon receiving said user input, comparing said user input and said electronic resource user access reference; and

granting access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said fourth series, identified with matching at least one numerical value of said first series with an equal numerical value in said third series, cross-referencing said matching equal value with a corresponding numerical value in said second series and selecting said corresponding numerical value of said second series as a numerical value of said fourth series.

In yet a further aspect of the present invention, a system for securing access to an electronic resource is provided, which comprises at least one data processing terminal, a first series of personal numerical values and a support including a second series of numerical values provided to a user, said terminal comprising storage means, processing means and display means, said storage means storing a combination of a user reference and an electronic resource user access reference for at least the said user and instructions which configure said processing means to

generate third and fourth series of random numerical values and request user input in response to said user requesting access to said electronic resource;

compare said user input and said electronic resource user access reference upon receiving said user input; and

grant access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said fourth series, identified with matching at least one numerical value of said first series with an equal numerical value in said third series, cross-referencing said matching equal value with a corresponding numerical value in said second series and selecting said corresponding numerical value of said second series as a numerical value of said fourth series.

According to a further aspect of the present invention, a support is provided for securing access to an electronic resource, said support comprising at least a second series of numerical values, said support being operationally positioned relative to the display device of a data processing terminal on which third and fourth series of numerical values are displayed in response to a user requesting access to an electronic resource, wherein said user is provided with a first series of personal numerical values and said support, whereby said user may match at least one numerical value of said first series with an equal numerical value in said third series, cross-reference said matching equal value with a corresponding numerical value in said second series and select said corresponding numerical value of said second series as a numerical value of said fourth series for granting access to said electronic resource upon the

comparison of said user input and an electronic resource user access reference returning a match.

Brief Description of the Drawings

5 The above and other features and advantages of the present invention will be more clearly understood from the following detailed description taken in conjunction with the accompanying illustrations listed below:

Figure 1 illustrates an environment comprising a data processing terminal connected to a network, at which a user with a support may request access authentication according to the
10 present invention;

Figure 2 details the data processing terminal of *Figure 1*, including a display;

Figure 3 details the support of *Figure 1*;

Figure 4 details processing steps performed by the terminal of *Figures 1* and *2*, including a step of outputting a graphical user interface;

15 *Figure 5* provides a graphical illustration of the interface of *Figure 4*;

Figure 6 provides a graphical illustration of the interface of *Figure 4* overlaid with the support of *Figures 1* and *3*;

Figure 7 provides a graphical illustration of the interface of *Figure 4* overlaid with the support of *Figures 1* and *3* according to an alternative embodiment of the present invention; and

20 *Figure 8* details processing steps performed by a remote terminal and the terminal of *Figures 1* to *6* in an alternative embodiment of the present invention.

Figure 9 details a further embodiment of the support of *Figure 1*;

Figure 10 provides a graphical illustration of the interface of *Figure 4* for use with the support of *Figure 9*;

25 *Figure 11* provides a graphical illustration of the interface of *Figure 10* overlaid with the support of *Figure 9*; and

Figure 12 provides a graphical illustration of the interface of *Figure 11* overlaid with the support of *Figures 9* and *11* in which a user makes a selection.

Detailed Description of the Drawings

30 An environment is shown in *Figure 1*, in which a user 101 is equipped with a support 102 provided by a support issuer 103 and may use a first computer terminal 104, for instance a personal computer located at the dwelling or workplace of user 101.

In an alternative embodiment of the present invention, user 101 may use a second computer terminal 105, for instance if terminals 104 and 105 are made available to users in a public access location, such as a library, or if terminals 104 and 105 are workplace terminals which user 101 may use alternatively. In the alternative embodiment, terminal 104 is optionally
5 connected to terminal 105 via a Local Area Network (LAN) 106, which may be implemented as either a wired Ethernet connection or a wireless Ethernet connection (WLAN), known to those skilled in the art as a Wi-Fi network.

Terminal 104 is optionally connected to a Wide Area Network (WAN) such as the Internet
10 107 via an Internet Service Provider (ISP) 108, to which it connects via any of a low-bandwidth dial-up modem connection or a high-bandwidth cable or Asynchronous Digital Subscriber Line (ADSL) connection 109. In an alternative embodiment, terminal 105 is likewise optionally connected to the Internet 107, for instance with sharing the connection 109 of terminal 104 to ISP 108 over the LAN or WLAN 106.

15 In yet another alternative embodiment of the present invention, a terminal 110 is located at support issuer 103 and is also connected to the Internet 107.

Therefore, depending upon the particular embodiment of the present invention, terminal 104
20 may be used as a local data processing system only, or as a locally network-connected (106) data-processing system only, or as a data-processing system connected to a plurality of wide and local networks (106, 107), in which embodiment terminal 104 may communicate data to terminal 110 and receive data therefrom.

25 An example of the terminal 104 shown in Figure 1 is provided in Figure 2. In the example, the respective architectures of terminals 104, 105 and 110 are substantially similar, for the sake of not unnecessarily complicating the present description, but it will be readily apparent to those skilled in the arts that the invention may not be limited to the example terminal described below.

30 Terminal 104 is a computer terminal configured with a data processing unit 201, data outputting means such as video display unit (VDU) 202, data inputting means such as a keyboard 203 and a pointing device (mouse) 204, data inputting/outputting means such as an optional modem connection 205A to network 107 or an optional Ethernet connection 205B
35 and to LAN 106 and optionally also to the Internet 107, a first reader/writer 206A for reading

data from and writing data to magnetic data-carrying medium 206B, and a second reader/writer 207A for reading data from and writing data to optical data-carrying medium 207B.

5 Within data processing unit 201, a central processing unit (CPU) 208, such as an Intel Pentium 4 manufactured by the Intel Corporation, provides task co-ordination and data processing functionality. Instructions and data for the CPU 208 are stored in main memory 209 and a hard disk storage unit 210 facilitates non-volatile storage of data and data processing applications. Network connection 205A is provided by way of a 56k or ADSL
10 modem 211 as a wired connection to the Internet 107. Network connection 205B is provided by way of a Network Interface Card (NIC) 212 as a wired or wireless connection to terminal 105 and optionally to the Internet 107.

A universal serial bus (USB) input/output interface 213 facilitates connection to the keyboard
15 and pointing devices 203, 204 and a further serial or parallel input/output interface 214 is provided for legacy purposes.

All of the above devices are connected to a data input/output bus 215, to which said magnetic data-carrying medium reader/writer 206A and optical data-carrying medium reader/writer
20 207B are also connected. A video adapter 216 receives CPU instructions over said bus 213 for outputting processed data to VDU 202.

In the embodiment, data processing unit 201 is of the type generally known as a compatible Personal Computer ('PC'), but may equally be any device configured with processing means,
25 output data display means, memory means, input means and wired or wireless network connectivity.

The support 102 issued to user 101 by support issuer 103 is further detailed in Figure 3. The support 102 takes the form of a card, preferably made of a durable plastic material and the
30 dimensions of which are substantially identical to a standard credit card. In the preferred embodiment of the present invention, support issuer 103 issues the card 102 with at least a first series of numerical values 301 and a second series of numerical values 302.

In an alternative embodiment of the present invention shown as a card 102B, the card 102B is configured with a see-through portion 303, located substantially between the first and second
35 series of numerical values 301, 302.

Each of the first and second series of numerical values 301, 302 preferably comprises an identical number of numerical values, which is 10 in the example but may be a higher or a lower number. Each of the values themselves are preferably randomly selected between 0
5 (zero) and 9 (nine), and each of the series 301, 302 is preferably generated as a random series, of 10 randomly-selected values in the example.

In the preferred embodiment of the present invention, the combination of the first and second series 301, 302 forms an encryption and decryption key, stored in a database the terminal 104
10 with information data of user 101, comprising at least a user reference and an electronic resource user access reference, for instance a user name and a access password respectively, when said support 102 is created and issued to user 101.

In an alternative embodiment of the present invention, the combination of the first and second
15 series 301, 302 forming the encryption and decryption key and information data of user 101, comprising at least a user reference and an electronic resource user access reference, for instance a user name and a access password respectively, stored in a remotely-accessible database in the terminal 110 when said support 102 is created and issued to user 101.

20 In another alternative embodiment of the present invention, shown as card 102C, support issuer 103 is a financial institution and that the card 102C is configured for use as a transaction card, e.g. a credit or debit card to effect payments and/or currency withdrawals, and so is further configured with a magnetic data-carrying strip 304. Further embodiments contemplate the inclusion of a chip (not shown) to configure card 102, 102B or 102C as a
25 smartcard.

Figure 4 details processing steps performed by the terminal 104 for requesting and obtaining access authorization to an electronic resource stored therein. In the preferred embodiment, terminal 104 stores instructions in storage means 210 which are loaded into RAM 209 and
30 processed by CPU 208 when the user 101 inputs data via keyboard or pointing device 203, 204 to signify a request to access an electronic resource at step 401, for instance a database stored in storage means 210 or an application to process same and likewise stored in storage means 210 and which will be loaded into RAM 209 and processed by CPU 208 upon user 101 being granted the requested access authorization. The instructions comprise a system module

and a random number generator as well as processing user input and the previously-described database, which retains key data and information data relating to user 101.

Upon receiving the user input of step 401, the system module is engaged and generates a third series of random numbers with respective values between 0 and 9, using the random number generator, at step 402. The third series preferably includes the same number of values as the first and second series 301, 302, e.g. 10. The instructions record the generated numbers and, with reference now to Figure 5, output a user interface 501 at step 403. The interface 501 presents the third series of numbers 502 and a plurality of user-selectable buttons, some of which are located in the interface to compliment the use of the support 102. Preferably, a button 503 is generated for each of the numbers of the third series 502, which is substantially vertically aligned therewith. Other buttons include a 'submit' button 504 and a 'cancel' button 505 and the interface further comprises a text input area 506 for user 101 to input a respective user reference as well as a cipher input area 507 for the instructions to input the enciphered user electronic resource user access reference according to the user interaction with the buttons 503.

At step 404, the user 101 inputs respective user reference data via keyboard and/or pointing device 203, 204 into the text input area 506 and interacts with the buttons 503. With reference now to Figure 6, the user manipulates the support 102 relative to VDU 202 so that each number of the first series 301 is substantially vertically aligned with a corresponding number of the third series 502 and the respective configuration of the support 102 and the interface 505 complement one another in such a way as to likewise substantially vertically align each number of the second series 302 with a corresponding button 503.

At step 404 still, the user recalls the first number of a respective electronic resource user access reference and locates the corresponding number 601 in the first series 301. In the example, the first number is "5" and, vertically adjacent to the number 5 is the corresponding number 602 in the third series 502, which is "1".

Having identified the number "1", the user 101 compares this number with the second series 302 to locate a number 603 having a corresponding "1" value therein and selects the button 503, 604 immediately above the number "1". The button is preferably assigned a value other than 1 within the system module. The user repeats this above sequence until the entire electronic resource user access reference is input, e.g. all 10 numbers of the user's respective

electronic resource user access reference have been enciphered. On completion of the enciphering of the electronic resource user access reference, the user submits the screen to the system module for processing by the instructions with selecting the "submit" button 504.

- 5 The instructions retrieve the username and ciphered password string presented by the user 101 via the software module and attempt to identify the validity of the username with processing the database, resulting in a first question asked at step 405, as to whether the username has been matched in said database. If the question of step 405 is answered negatively, the instructions output an error message at step 409 and call upon the module to
10 output a new third series 502 and interface at step 402.

- Alternatively, the question of step 405 is answered positively, i.e. the username is valid, and at step 406 the instructions select the value of the first element of the enciphered user access reference, assign this value to a memory variable – offset and examine the first series 301 at
15 the index indicated by the offset variable, and retrieve the value contained therein from the database. The retrieved value is recorded in the memory variable offset1. The instructions then examine the value contained in the second series 302 at index offset1. This constitutes the first deciphered number of the user access reference string. This process continues until completion and the now-entirely deciphered user access reference string is compared against
20 the corresponding user access reference stored in the database, whereby a second question asked at step 407, as to whether the user access reference has been matched in said database. If the question of step 407 is answered negatively, the instructions output an error message at step 409 and call upon the module to output a new third series 502 and interface at step 402.

- 25 Alternatively, the question of step 407 is answered positively, i.e. the user access reference name is valid, and at step 408 the instructions route the user to the requested electronic resource, i.e. the requested access to the electronic resource is granted.

- An alternative embodiment of the present invention is illustrated in Figure 7, in which the
30 support 102 comprises a see-through portion 303 and the interface 501 is configured by the module so that the third series 502 of values can be overlaid with the see-through portion 303 when the user manipulates the support 102 relative to VDU 202, so that each number 601 of the first series 301 on support 102 is substantially vertically aligned with a corresponding number 602 of the third series 502, which number 602 on display 202 is directly observable
35 relative to said corresponding number 601 through the transparent portion 303. Further

alternative embodiments contemplate respective see-through portions 303 for each number of the third series 502.

An alternative embodiment of the present invention is shown in Figure 8, in which the terminal 110 of support supplier 103 is a remote server and the key data 301, 302, user reference and electronic resource user access reference are stored in a database which is itself stored at said server 110. In the Figure, a portion of the processing steps previously described in Figure 4 are performed by server 110, which is particularly useful when user 101 wants to access a remote electronic resource, for instance over the Internet 107, such as the website of the bank at which said user holds an account and which account may be remotely interacted with via said website, or the website of a retail concern at which said user may remotely effect purchases. The processing steps respectively performed by terminal 104 operated by user 101 are therefore represented as grouped within a logical block 701 and the processing steps respectively performed by server 110 upon user 101 inputting data at step 401 at terminal 104 to access a remote electronic resource are represented as grouped within a logical block 702.

In this alternative embodiment, the instructions are not stored at terminal 104 but are stored at server 110 from which, alternatively, either the system module is downloaded by terminal 104 as any of a browser plug-in, an Active-X plug-in, a Java script, a HTML script or the like further to user 101 performing step 401, or only the user interface 501 is downloaded by terminal 104. The distributed system is described in Figure 8 with data exchanged between remote terminals 104 and 108 over the Internet 107, but it will be readily apparent to those skilled in the art that the distributed system may equally be described in, and the invention extending to, the context of any network, including the example LAN 106.

In order to further improve the tamper-proofing of the authentication procedure according to the present invention, an alternative embodiment of the invention contemplates the use of four series of numerical values, wherein the first series 301 comprises personal numerical values and may be known as a Personal Identification Number (PIN) or a Personal Identification Code (PIC). Such a code is preferably provided to the user by support issuer 103 independently of the support 102 and in lieu of the password information data of user 101, and two examples of a support 102 issued to user 101 by support issuer 103 for use with this embodiment are illustrated in further details in Figure 9.

In this embodiment, support issuer 103 issues the support 102D with a grid configuration, wherein each cell or only certain cells of the grid include at least a second series of numerical values 302. The second series is preferably provided on the card in a variable and/or randomised manner, both in terms of grid location and in terms of numerical value: each cell
5 on the token can include a value that is single, two or three digits in length, such as 1, 23, 359, etc. and is generally comprised between 0 and 999. An alternative embodiment of support 102D is also shown as 102E and includes a magnetic stripe 304, as previously described above. Further embodiments also contemplate the inclusion and use of a microprocessor (CHIP) in relation to supports 102D, 102E. In an alternative embodiment of the present
10 invention, the supports 102D, 102E are again configured with a see-through portion 303, for instance substantially all of the grid area of supports 102D, 102E and in which the second series of values 302 is printed on the see-through portion.

In this embodiment and in accordance with the present invention and the description of Figure
15 4, upon receiving the user input of step 401, the system module is engaged and generates a third series of random numbers, with each of the numbers having a respective value between 0 and 9 in the example, using the random number generator, at step 402. The third series preferably includes the same number of values as the first series 301, e.g. 10. The instructions record the generated numbers and, with reference now to Figure 10, output a user interface
20 1001 at step 403, which presents the third series of numbers 1002.

In an alternative embodiment, which is shown in the Figure, the third series of numbers 1002 is generated as both an horizontal 1002A and a vertical 1002B series of random numerical values, which configuration may then be used as a grid coordinate system. It will however be
25 readily apparent to those skilled in the art that this grid configuration is optional, as only the horizontal 1002A series of random numerical values is required to work the particular embodiment first discussed in relation to Figure 9, as the core is that a user having a PIN, looks to the user interface 1001 for the digits of that PIN in the third series 1002A in turn, which indicates a cell on their token 102D that contains a value 302 that is entered in place of
30 that PIN number.

Irrespective of whether the third series of random numbers is generated as only the horizontal series 1002A, or both the horizontal and the vertical series 1002A, 1002B, the system module is still engaged and generates a fourth series of random numbers, each of the numbers having
35 a value between 0 and 5, using the random number generator, at step 402 still. The fourth

series is represented on the user interface 1001 with user-selectable buttons 1003, which may be presented in sequential fashion or randomly.

Importantly, the buttons 1003 are labeled with a value comprised between 0 and 9, but the
5 actual value input when the user 101 selects any of the buttons 1003 is a corresponding random value between 0 and 5 of the fourth series, as generated and assigned by the random number generator at step 402. Thus, for instance, selecting the leftmost button labeled '0' first may result in the inputting of a first value equal to 0, 1, 2, 3, 4 or 5 in access identifier 507. Likewise, selecting the next-to-leftmost button labeled '1' may result in the inputting of a
10 second value equal to 0, 1, 2, 3, 4 or 5 in access identifier 507, and so on and so forth.

Other buttons include the 'submit' button 504 and the 'cancel' button 505 and the interface further comprises the text input area 506 for user 101 to input a respective user reference as well as the cipher input area 507 for the instructions to input the enciphered user electronic
15 resource user access reference according to the user interaction with the buttons 1003.

In this embodiment and in accordance with the present invention and the description of Figure 4, the user 101 inputs respective user reference data via keyboard and/or pointing device 203, 204 into the text input area 506 and interacts with the buttons 1003 at step 404. With
20 reference now to Figure 11, the user recalls the first number of the first series of personal numerical values, for instance '0', and matches the corresponding, equal number '0' (1101) in the third series 1002 therewith, in order to cross-reference a number 1102 of the second series 302. Depending upon the embodiment, the location of the corresponding, equal number '0' (1101) may be in the (horizontal) series 1002 only, or the user may additionally locate the
25 corresponding, equal number '0' (1101B) in the vertical third series 1002B (embodiment shown). Thus, depending upon the embodiment, the cross-referencing of the number 1102 of the second series 302 may be realized, respectively, either with observing which value 1102 of the series 302 on the support 102 is located directly underneath the corresponding equal number '0' (1101) in the (horizontal) series 1002, in this latter case '5' in the example., or
30 observing which value 1103 of the series 302 on the support 102 is located at the intersection between the corresponding equal numbers '0' 1101A and 1101B in the horizontal and vertical third series 1002A, 1002B in the grid coordinate system, in this latter case '7' in the example.

A further embodiment contemplates receiving an indication of at least a second numerical
35 value of the first series 301 for matching with a corresponding equal numerical value in the

vertical series 1002B of the third series of random numerical values, wherein this second numerical value may be the same corresponding equal number '0' 1101B of the example, or a second, different number 1101C of the first series 301, in the example '5'. In the latter case, the cross-referencing yields the value '94' (1104) in the example. This indication may be
5 received by the user 101 from a local or remote source, such as a mobile telephone handset, a pager, a network-connected terminal, a dongle input/output device and a set of instructions such as a plug-in application or an applet. For instance, in the case of an embodiment involving remote terminal 110 of support issuer 103, this terminal 103 may initiate the sending of the indication when the user first performs step 401, via any appropriate data
10 communication means.

Thus, and irrespective of the embodiment considered, the user cross-references the numerical value of the third series 1002, 1002A, 1002B matching the numerical value of the first series 301, with the second series 302 on the support 102 for a corresponding number 1102, 1103,
15 1104 of the said second series. With reference now to Figure 12, having located the corresponding number 1201 of the said second series 302 on the support 102, the user then selects a button 1202 labeled with a numerical value of the fourth series 1003 corresponding to the located numerical value 1201, whereby the actual value input is a corresponding random value between 0 and 5 of the fourth series as previously described. In the example,
20 the random value generated and assigned to button '7' by the random number generator at step 402 is 3 and therefore results in the inputting of the value 3 in access identifier 507.

The user repeats this above sequence until the entire first series of personal numerical values is input, e.g. all numbers of the user's PIN have been enciphered. On completion of the
25 enciphering of the electronic resource user access reference, the user submits the screen to the system module for processing by the instructions with selecting the "submit" button 504. In a particularly advantageous implementation of this embodiment, the accumulated content of the user access identifier 507 is further secured through hash to produce cipher text for transmission over the network, or any other industry-standard enciphering technique.

30

As previously described, the instructions retrieve the username and ciphered password string presented by the user 101 via the software module and attempt to identify the validity of the username with processing the database, resulting in a first question asked at step 405, as to whether the username has been matched in said database. If the question of step 405 is
35 answered negatively, the instructions output an error message at step 409 and call upon the

module to output a new third series 1002 and interface at step 402, or simply to reissue the previously-failed challenge.

Alternatively, the question of step 405 is answered positively, i.e. the username is valid, and at step 406 the instructions interrogate the first series for a digit of the personal identification code as required by the system producing the variable offset1. The instructions then identify the intersecting value of the second series 302 of numerical values from the support 102D relative to the position of offset1 in the row of the third series of numerical values as identified by the criteria of the system, whereby for each identified value of the variable series retrieved, the assigned value of the third series is applied. The instructions then process the combined fourth series numerical values entered in the access identifier 507 with an identical hash algorithm as presented in the user interface 501, and the cipher text received at submission is compared to the cipher text as generated for a match.

This process continues until completion and the now-entirely deciphered user access reference string is compared against the corresponding user access reference stored in the database, whereby a second question asked at step 407, as to whether the user access reference has been matched in said database. If the question of step 407 is answered negatively, the instructions output an error message at step 409 and call upon the module to output a new third series new third series 1002 and interface at step 402, or simply to reissue the previously-failed challenge.

Alternatively, the question of step 407 is answered positively, i.e. the user access reference name is valid, and at step 408 the instructions route the user to the requested electronic resource, i.e. the requested access to the electronic resource is granted.

The present invention therefore improves the security of access authentication required for a user to access an electronic resource, whether locally or via a network, by decreasing the risk of compromising authentication data. with filtering a user access reference, such as a password. The password is altered into another numeric state and this altered numeric state is further interpreted, the interpreted result being entered into the user interface. A user attempting to gain unauthorised access to a local or remote electronic resource, such as personal information of a different user, would need to be in possession of all three factors, the password, the support 102 and the interactive user interface 501 to gain successful access.

The present invention provides a Multiple Factor Authentication solution, which confers a high level of confidence to password- or PIN-based security. According to the present invention, a user's password is never directly transacted against, or disclosed over networks such as the Internet. The invention solves the problem of users being offered fake screens by users practicing Phishing attacks. If an unauthorized user mimics the genuine interface 501, this interface will offer no hint as to the password or construction of the support 102. If the user is deceived into putting genuine data into an interface 501 developed by an unauthorized user, then that data alone will not suffice to gain genuine access to the targeted electronic resource.

10

The present invention thus manages the security of the access authorization process without regard or concern for the environment to which it is connected, namely a computer, or through which it is communicated, namely a network.

15 The words "comprises/comprising" and the words "having/including" when used herein with reference to the present invention are used to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

Claims

1. A method of securing access to an electronic resource at a user terminal equipped with a display device, the method comprising the steps of:
 - 5 providing a user with a first series of personal numerical values and with a second series of numerical values on a support;
 - storing a combination of a user reference and an electronic resource user access reference for said user;
 - in response to said user requesting access to said electronic resource,
 - 10 generating third and fourth series of random numerical values and requesting user input ;
 - upon receiving said user input, comparing said user input and said electronic resource user access reference; and
 - granting access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said fourth series, identified
 - 15 with matching at least one numerical value of said first series with an equal numerical value in said third series, cross-referencing said matching equal value with a corresponding numerical value in said second series and selecting said corresponding numerical value of said second series as a numerical value of said fourth series.
- 20 2. The method of claim 1, wherein each value of said second series of numerical values is comprised between 0 and 999 and is provided randomly on said support.
3. The method of claim 1 or 2, wherein said second series of numerical values on a support is configured as a grid.
- 25 4. The method of claim 3, wherein the step of generating said third series of random numerical values includes the further step of generating said third series as both an horizontal and a vertical series of random numerical values that may be used as a grid coordinate system.
- 30 5. The method of claim 4, wherein the step of matching at least one numerical value of said first series with an equal numerical value in said third series includes the further step of matching at least one numerical value of said first series with an equal numerical value in both the horizontal and the vertical series of random numerical values.

6. The method of claim 5, comprising the further step of receiving an indication of at least a second numerical value of said first series for matching with an equal numerical value in the vertical series of random numerical values.
- 5 7. The method of claim 6, wherein the indication of at least a second numerical value of said first series is received from a local or remote source selected from the group comprising a mobile telephone handset, a pager, a network-connected terminal, a dongle input/output device and a set of instructions such as a plug-in application or an applet.
- 10 8. The method of any of claims 5 to 7, wherein the step of cross-referencing said matching equal value or values of said third series with a corresponding numerical value in said second series includes the further step of looking up the numerical value in said second series corresponding to the intersection between the matched horizontal and vertical equal numerical values in the grid coordinate system.
- 15 9. The method of any of claims 1 to 8, wherein the step of generating said third and fourth series of random numerical values includes the further step of outputting said third and fourth series on a display, the step of requesting user input includes the further step of prompting said user to input data on said display, and the step of identifying at least one
- 20 numerical value of said fourth series includes the further step of positioning the support relative to the display to facilitate the identification.
10. The method of claim 9, wherein said support further comprises at least one substantially see-through portion.
- 25 11. The method of any of claims 1 to 10, wherein the first series is a personal identification number (PIN) or code (PIC).
- 30 12. A system for securing access to an electronic resource comprising at least one data processing terminal, a first series of personal numerical values and a support including a second series of numerical values provided to a user, said terminal comprising storage means, processing means and display means, said storage means storing a combination of a user reference and an electronic resource user access reference for at least the said user and instructions which configure said processing means to

generate third and fourth series of random numerical values and request user input in response to said user requesting access to said electronic resource;

compare said user input and said electronic resource user access reference upon receiving said user input; and

5 grant access to said electronic resource upon said comparison returning a match,

wherein said user input comprises at least one numerical value of said fourth series, identified with matching at least one numerical value of said first series with an equal numerical value in said third series, cross-referencing said matching equal value with a corresponding numerical value in said second series and selecting said corresponding
10 numerical value of said second series as a numerical value of said fourth series.

13. The system of claim 12, wherein each value of said second series of numerical values is comprised between 0 and 999 and is provided randomly on said support.

15 14. The system of claim 12 or 13, wherein said second series of numerical values on a support is configured as a grid.

15. The system of claim 14, wherein said instructions further configure said processing means to generate said third series as both an horizontal and a vertical series of random
20 numerical values that may be used as a grid coordinate system.

16. The system of claim 15, wherein said user matches at least one numerical value of said first series with an equal numerical value in both the horizontal and the vertical series of random numerical values.

25 17. The system of claim 16, wherein said instructions further configure said processing means to receive an indication of at least a second numerical value of said first series for matching with an equal numerical value in the vertical series of random numerical values.

30 18. The system of claim 17, wherein said terminal further comprises communication means and said instructions further configure said processing means to receive the indication of at least a second numerical value of said first series from a local or remote source selected from the group comprising a mobile telephone handset, a pager, a network-connected terminal, a dongle input/output device and a set of instructions such as a plug-in application or
35 an applet.

19. The system of any of claim 16 to 18, wherein said user looks up the numerical value in said second series corresponding to the intersection between the matched horizontal and vertical equal numerical values in the grid coordinate system.

5

20. The system of any of claims 12 to 19, wherein said instructions further configure said processing means to output said third and fourth series on said display means, to prompt said user to input data on said display, and the user may position the support relative to the display to facilitate the identification.

10

21. The system of claim 20, wherein said support further comprises at least one substantially see-through portion.

15

22. The system of any of claims 12 to 21, wherein the first series is a personal identification number (PIN) or code (PIC).

20

23. A support for securing access to an electronic resource, said support comprising at least a second series of numerical values, said support being operationally positioned relative to the display device of a data processing terminal on which third and fourth series of numerical values are displayed in response to a user requesting access to an electronic resource, wherein said user is provided with a first series of personal numerical values and said support, whereby said user may match at least one numerical value of said first series with an equal numerical value in said third series, cross-reference said matching equal value with a corresponding numerical value in said second series of said support and select said corresponding numerical value of said second series as a numerical value of said fourth series for granting access to said electronic resource upon the comparison of said user input and an electronic resource user access reference returning a match.

25

24. The support of claim 23, wherein each value of said second series of numerical values is comprised between 0 and 999 and is provided randomly on said support.

30

25. The support of claim 24 or 25, wherein said second series of numerical values on a support is configured as a grid.

26. The support of any of claim 23 to 25, wherein said third series is displayed as horizontal and vertical series of random values, said user looks up the numerical value in said second series of said support corresponding to the intersection between the horizontal and vertical values corresponding to the at least one numerical value of said first series matched
5 therewith.

27. The support of any of claims 23 to 26, wherein said data processing terminal is configured to prompt said user to input said data on said display, and the user may position the support relative to the display to facilitate the identification.
10

28. The support of claim 27, further comprising at least one substantially see-through portion.

29. A method of securing access to an electronic resource at a user terminal equipped with a display device, the method comprising the steps of:
15

providing a user with at least first and second series of numerical values on a support;

storing a combination of a user reference and an electronic resource user access reference for said user;

in response to said user requesting access to said electronic resource, generating a third series of random numerical values and requesting user input ;
20

upon receiving said user input, comparing said user input and said electronic resource user access reference; and

granting access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said first series identified with positioning said support relative to said display device and comparing corresponding
25 numerical value of said second series with corresponding numerical value of said third series.

30. A system for securing access to an electronic resource comprising at least one data processing terminal and a support including at least first and second series of numerical values, said terminal comprising storage means, processing means and display means, said
30 storage means storing a combination of a user reference and an electronic resource user access reference for at least one user and instructions which configure said processing means to:

generate a third series of random numerical values and request user input in response to said user requesting access to said electronic resource;

compare said user input and said electronic resource user access reference upon receiving said user input; and

grant access to said electronic resource upon said comparison returning a match, wherein said user input comprises at least one numerical value of said first series identified with positioning said support relative to said display device and comparing corresponding numerical value of said second series with corresponding numerical value of said third series.

31. A support for securing access to an electronic resource comprising at least first and second series of numerical values, said support being operationally positioned relative to the display device of a data processing terminal on which a third series of numerical values is displayed in response to a user requesting access to an electronic resource, wherein said user may compare corresponding numerical value of said second series of said support with corresponding numerical value of said third series and input at least one numerical value of said first series identified by said comparison for granting access to said electronic resource upon the comparison of said user input and an electronic resource user access reference returning a match.

32. The method of claim 29, the system of claim 30 or the support of claim 31, wherein said support further comprises at least one substantially see-through portion.

33. The method of claim 32, wherein the step of comparing corresponding numerical value of said second series with corresponding numerical value of said third series comprises the further step of positioning the see-through portion of the support over the third series on the display device.

34. The method of claim 29, the system of claim 30 or the support of claim 31, wherein the first, second and third series of numerical values may number ten numerical values, each of which is randomly comprised between 0 (zero) and 9 (nine).

35. The method of claim 29, the system of claim 30 or the support of claim 31, wherein the third series is generated as a random series to uniquely encrypt the electronic resource user access reference for every access authentication procedure.

36. The method of claim 29, the system of claim 30 or the support of claim 31, wherein the first, second and third series of numerical values are substantially spaced relative to one another both on the support and the display device, to facilitate the comparison therebetween.

5 37. The method of claim 29, the system of claim 30 or the support of claim 31, wherein the terminal is connected to a network and the electronic resource is a data resource stored at a first remote terminal.

38. The method, the system or the support of claim 37, wherein the combination of a user
10 reference and an electronic resource user access reference for said user is stored at a second remote terminal.

39. The method, the system or the support of claim 38, wherein the third series is
15 generated at said second remote terminal and communicated to the terminal of the user over the network.

40. A method of requesting access to an electronic resource at a user terminal equipped with a display device, the method comprising the steps of:

in response to said terminal outputting a third series of random numerical values on
20 said display device and requesting user input,

positioning a support having first and second series of random numerical values thereon relative to said first series of random numerical values on said display device;

inputting at least one numerical value of said first series identified with comparing
corresponding numerical value of said second series with corresponding numerical value of
25 said third series; and

submitting said input for requesting access to said electronic resource.

41. The method of claim 40, wherein said support further comprises at least one substantially see-through portion.

30

42. The method of claim 41, wherein said positioning comprises the further step of positioning the see-through portion of the support over the third series on the display device.

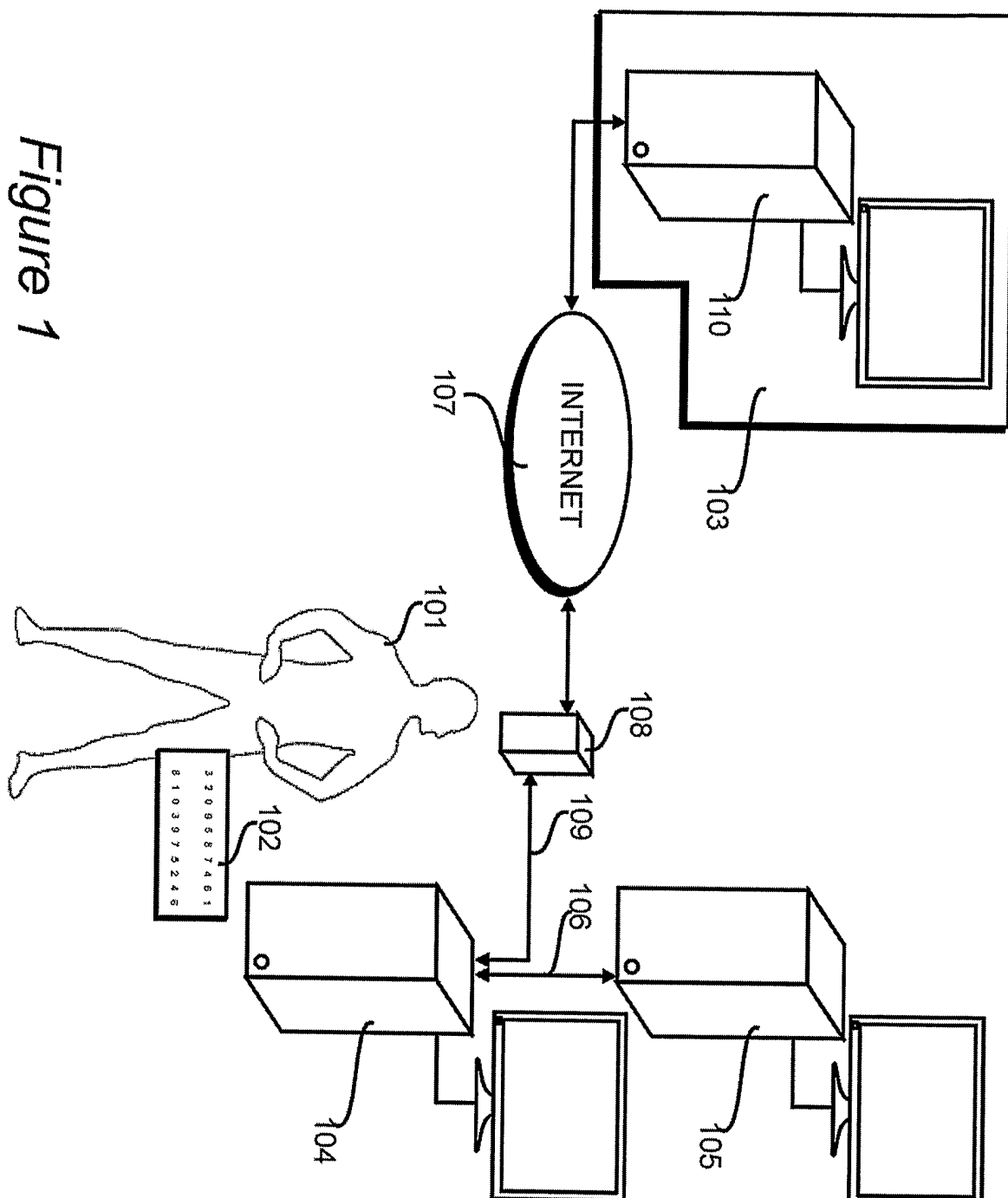
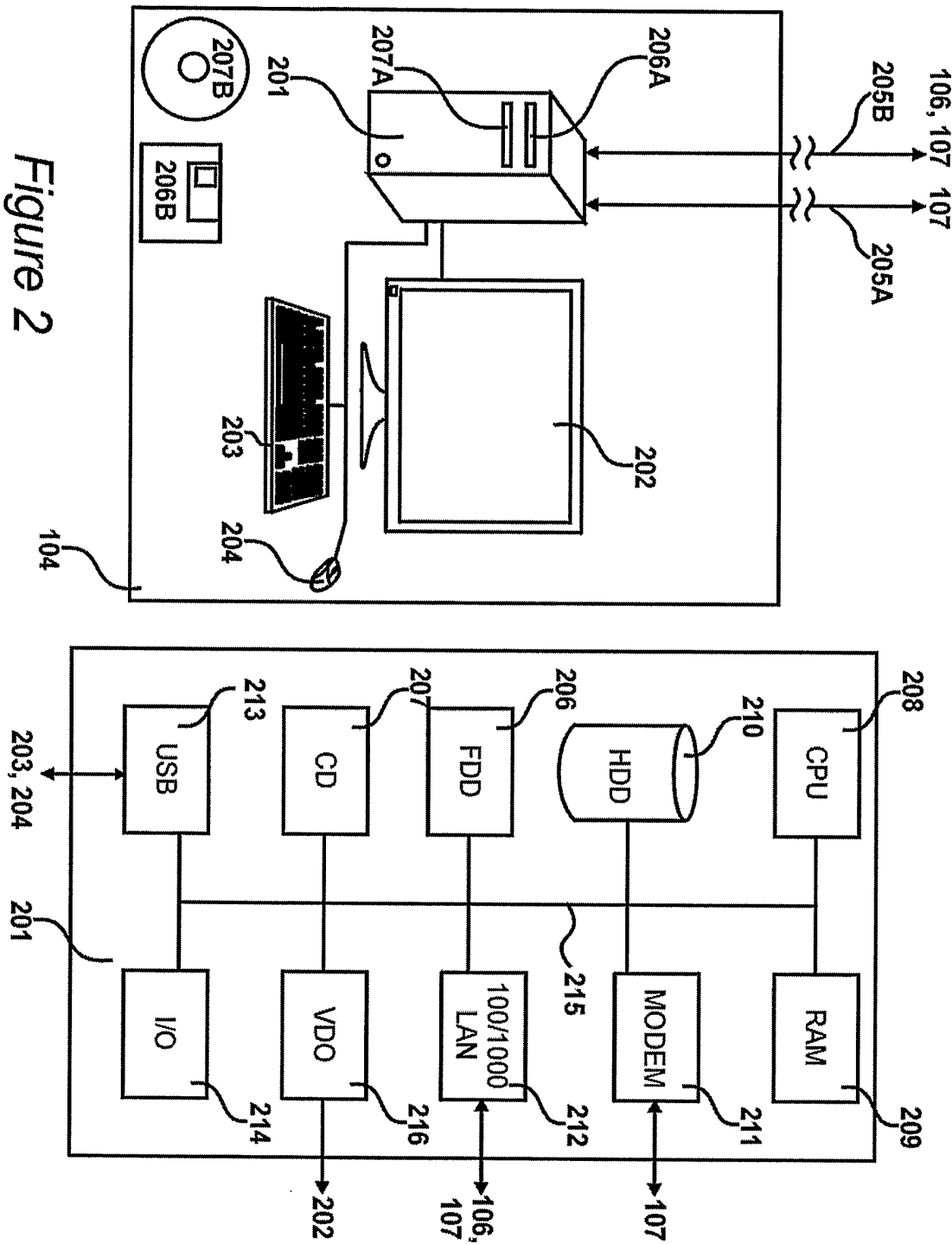


Figure 1



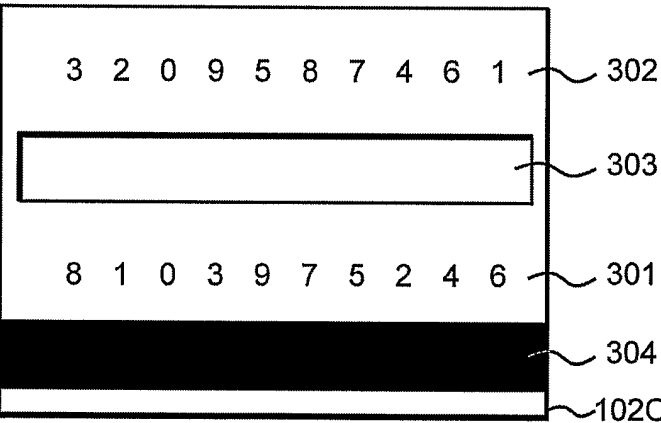
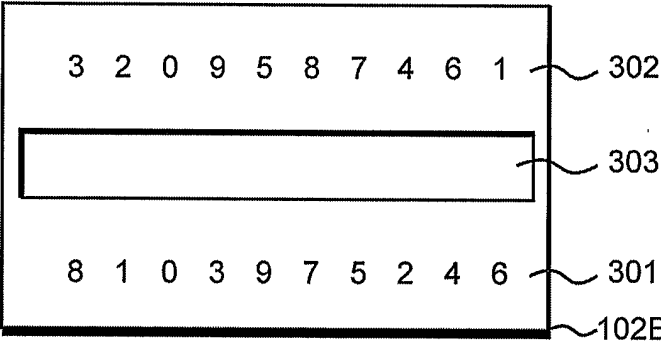
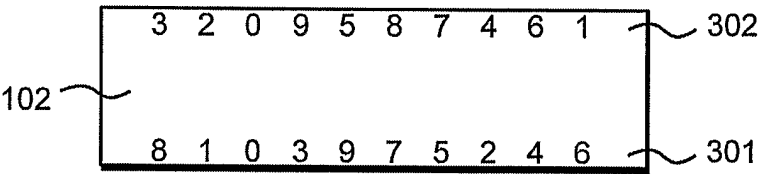
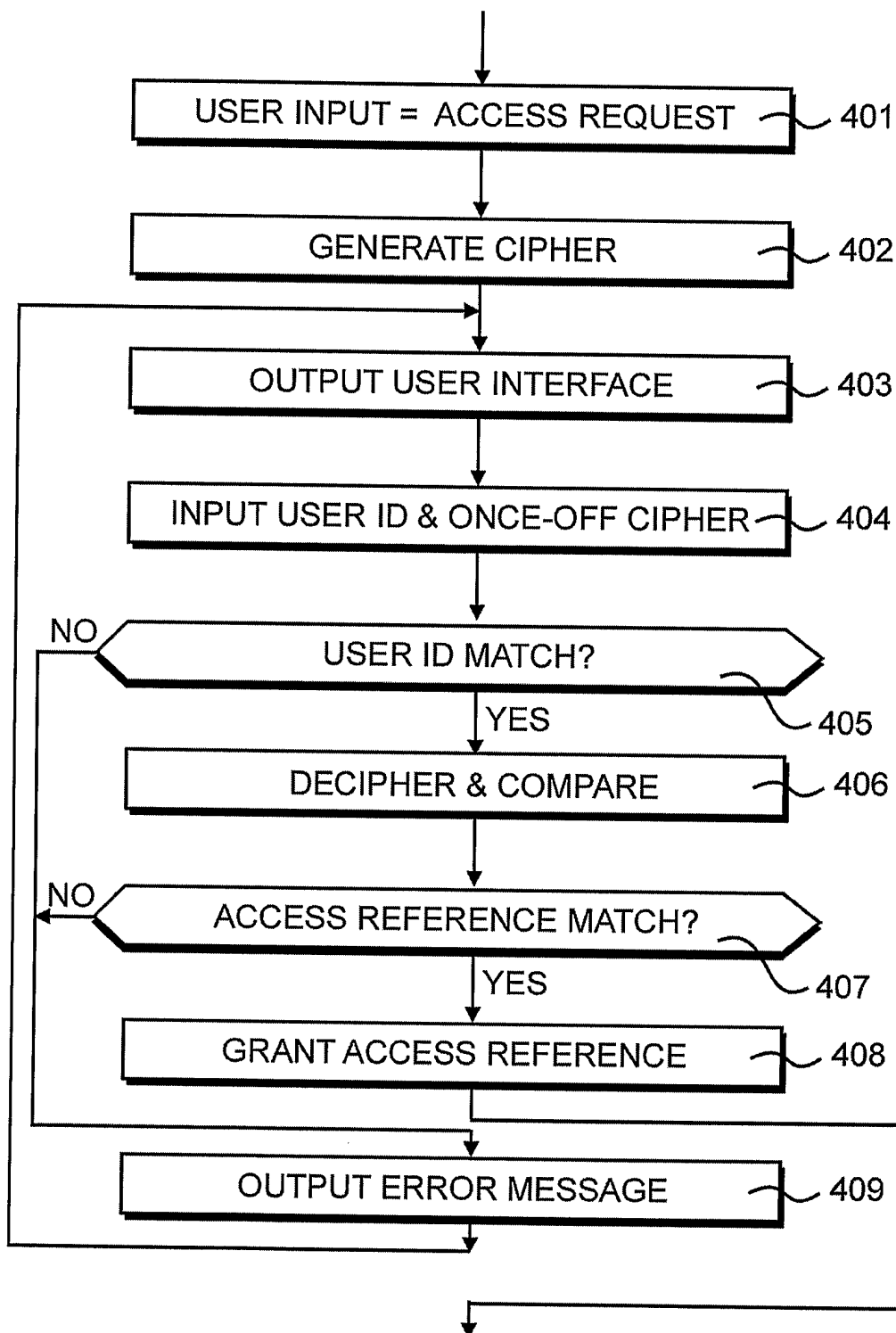


Figure 3

*Figure 4*

The diagram illustrates a user interface (202) within a larger frame (501). The interface is titled "USER INTERFACE". It contains the following elements:

- A label "USER IDENTIFIER:" followed by a text input field (506).
- A label "ACCESS IDENTIFIER:" followed by a text input field (507).
- A row of ten empty square boxes (503) for numeric input.
- A row of ten square boxes (502) containing the digits 4, 2, 7, 5, 6, 0, 1, 9, 3, and 8.
- A "SUBMIT" button (504) and a "CANCEL" button (505) at the bottom.

Figure 5

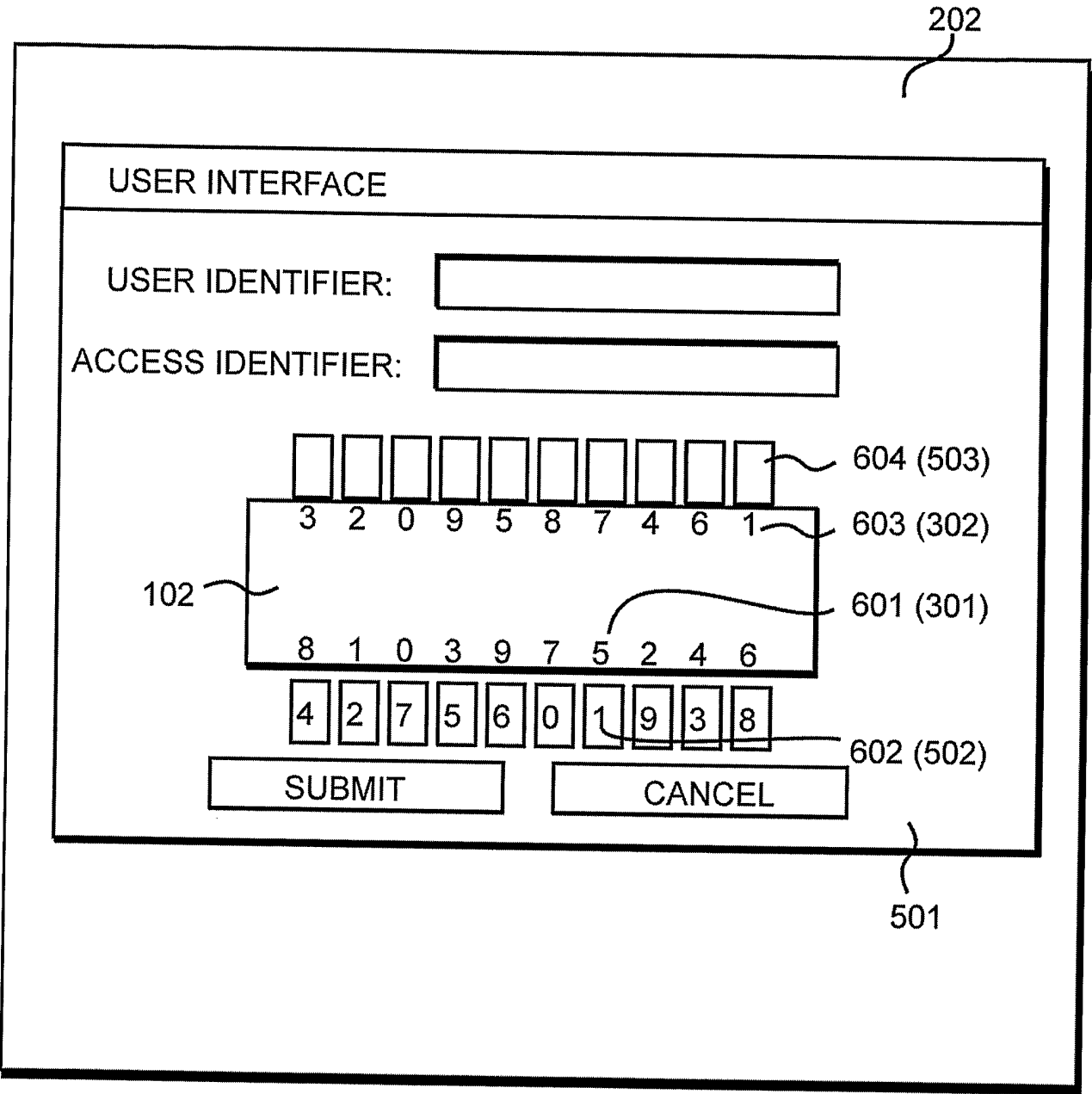


Figure 6

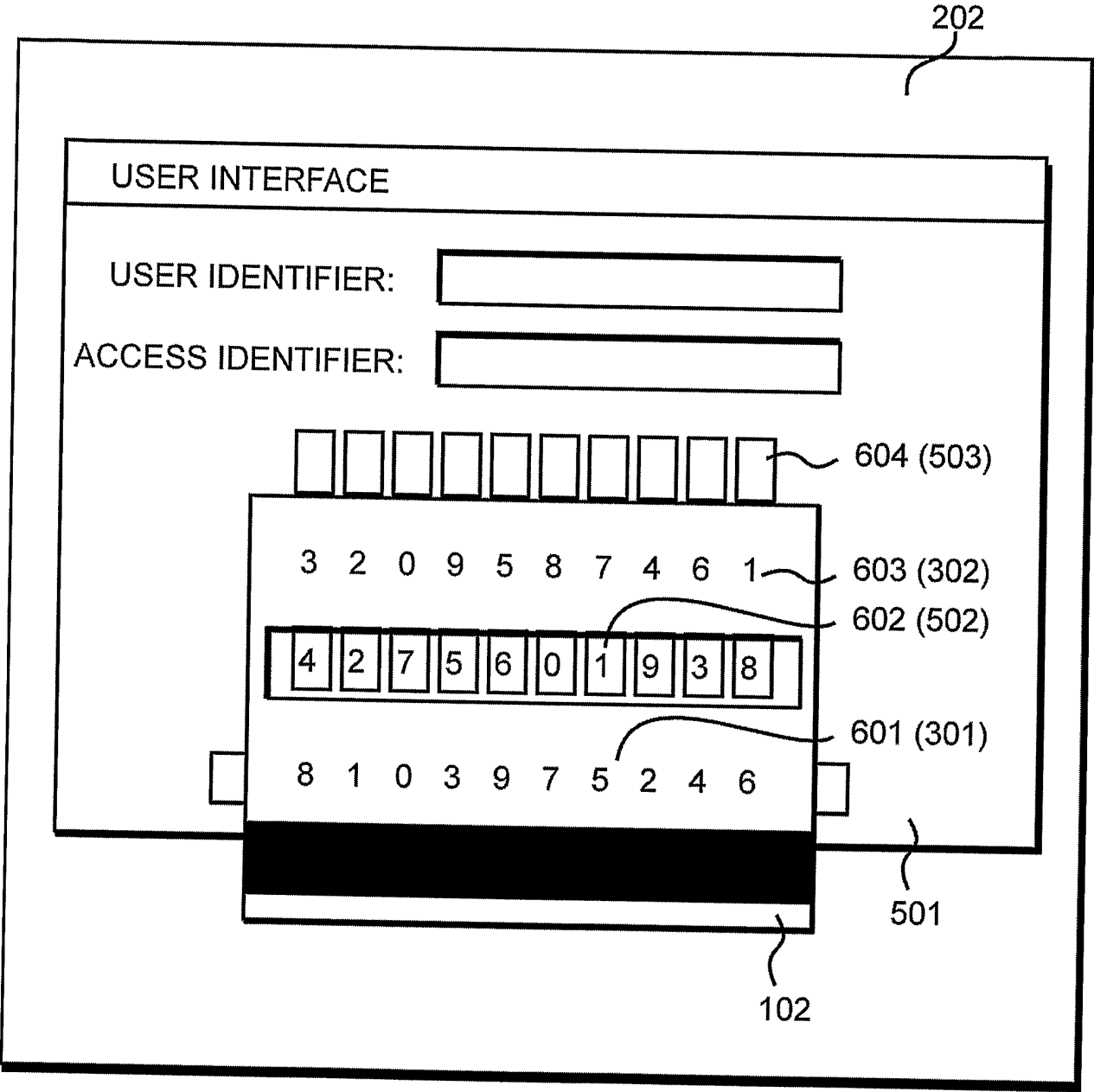
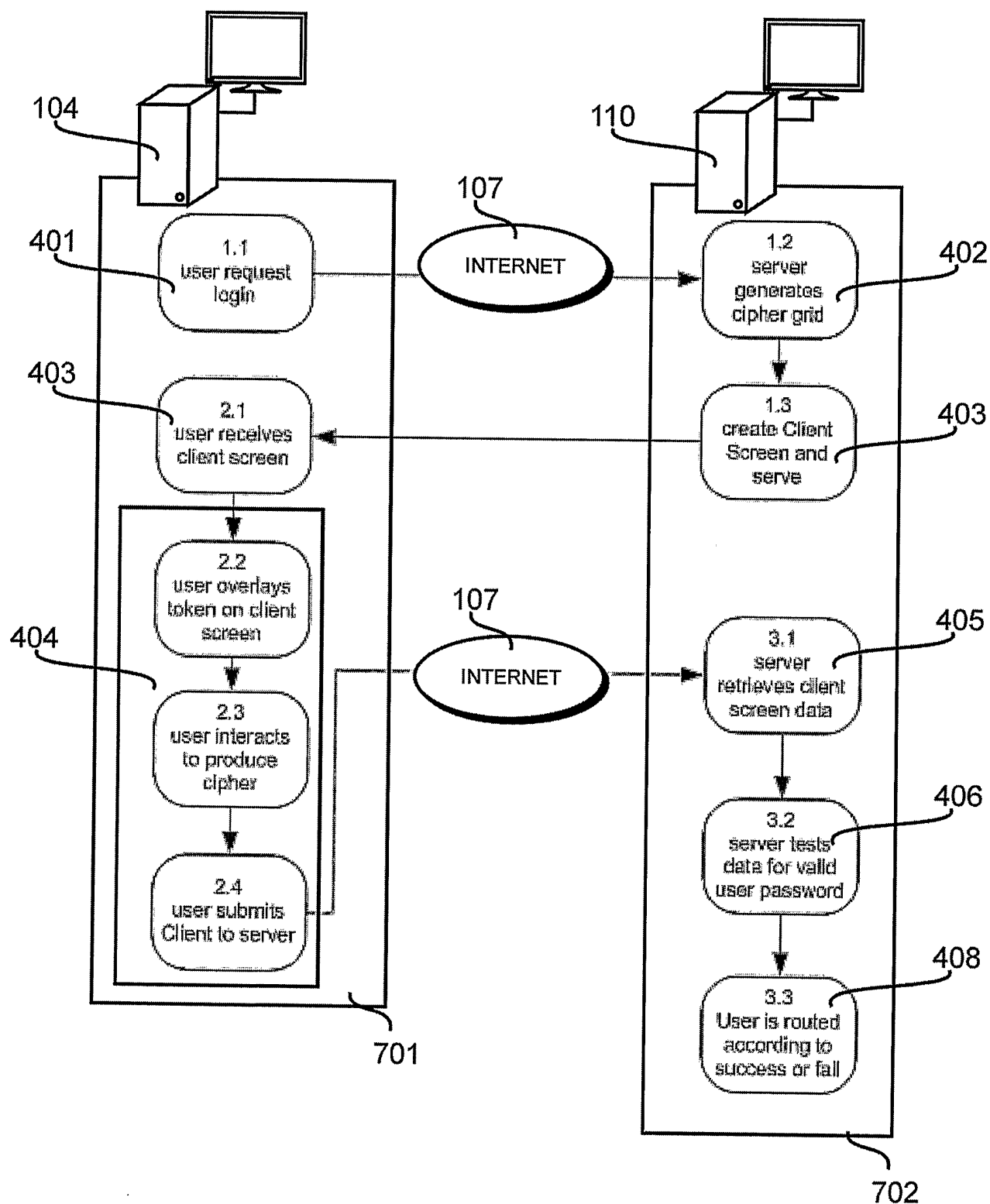


Figure 7

*Figure 8*

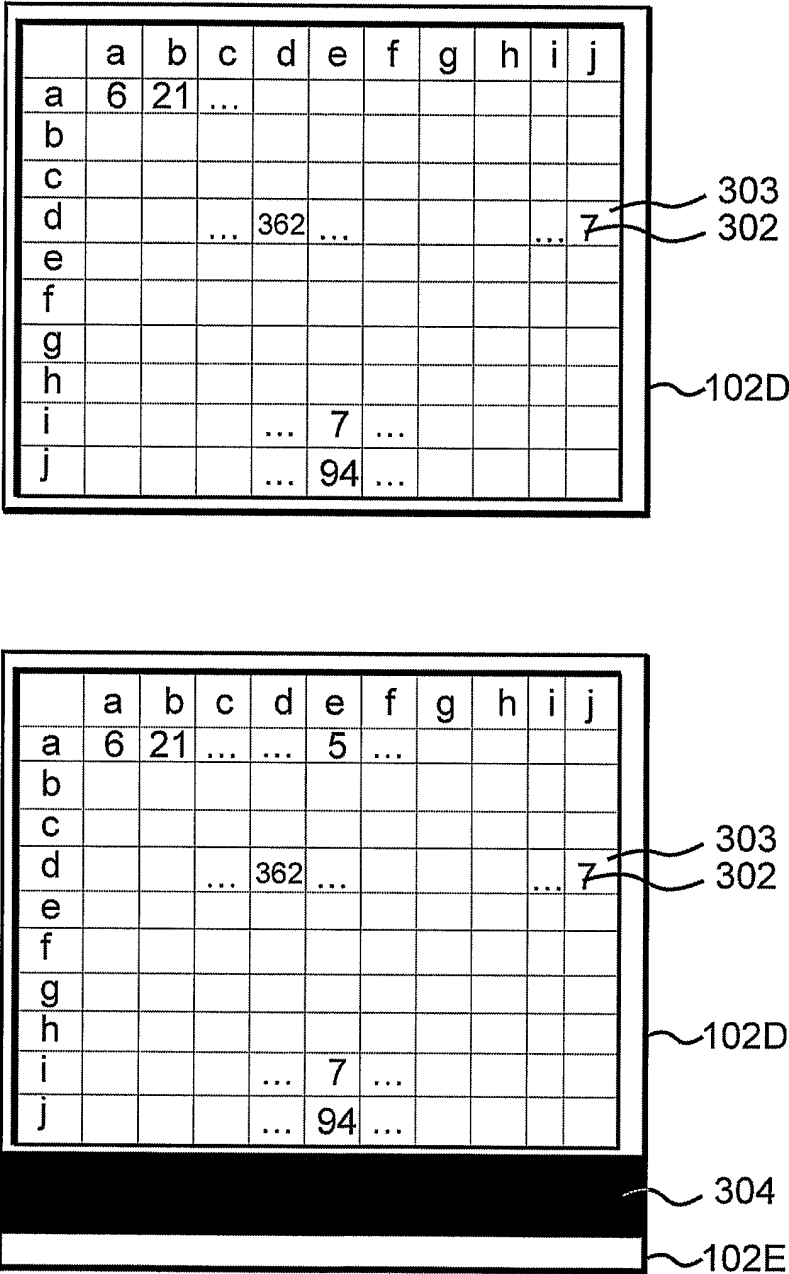


Figure 9

202
1001

USER INTERFACE

USER IDENTIFIER:

ACCESS IDENTIFIER:

0

1

2

3

4

5

6

7

8

9

		3	1	7	5	0	4	8	2	9	6
		a	b	c	d	e	f	g	h	i	j
1002B	6	a									
	4	b									
	1	c									
	3	d									
	2	e									
	8	f									
	9	g									
	7	h									
	0	i									
	5	j									

504 SUBMIT

CANCEL 505

1003
1002, 1002A

Figure 10

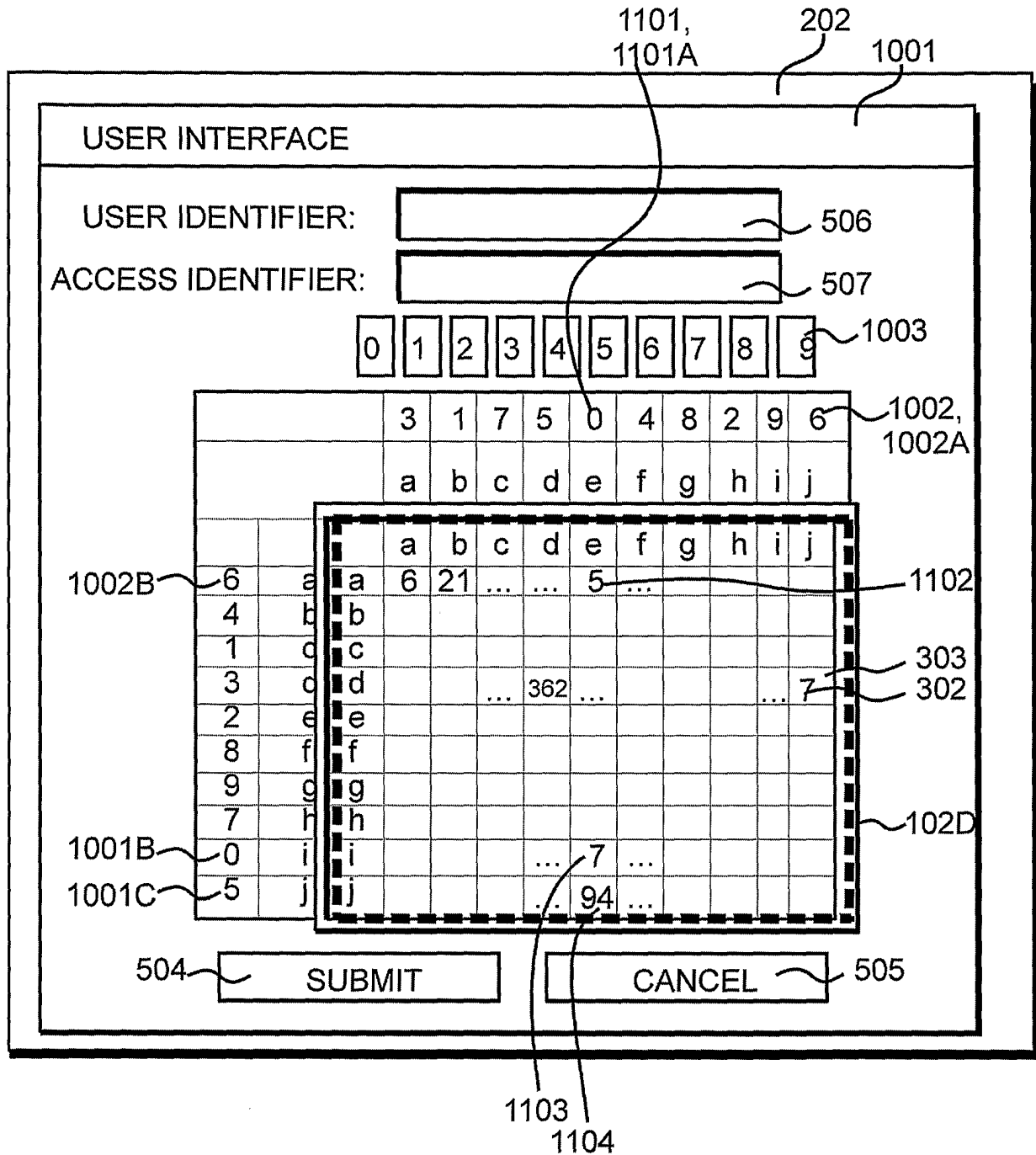


Figure 11

USER INTERFACE

USER IDENTIFIER:

ACCESS IDENTIFIER:

0 1 2 3 4 5 6 7 8 9

		3	1	7	5	0	4	8	2	9	6
		a	b	c	d	e	f	g	h	i	j

		a	b	c	d	e	f	g	h	i	j
6	a	a	6	21	...	...	5	...			
4	b	b									
1	c	c									
3	d	d			...	362	...			...	7
2	e	e									
8	f	f									
9	g	g									
7	h	h									
0	i	i			...	7	...				
5	j	j			...	94	...				

SUBMIT CANCEL

Figure 12