HU000032360T2

(19) **HU**

(11) Lajstromszám: **E 032 360**

(13) **T2**

MAGYARORSZÁG
Szellemi Tulajdon Nemzeti Hivatala

EURÓPAI SZABADALOM
SZÖVEGÉNEK FORDÍTÁSA

(21) Magyar ügyszám: **E 06 118042**
(22) A bejelentés napja: **2006. 07. 28.**

(96) Az európai bejelentés bejelentési száma:
EP 20060118042
(97) Az európai bejelentés közzétételi adatai:
EP 1755062 A2 **2007. 02. 21.**
(97) Az európai szabadalom megadásának meghirdetési adatai:
EP 1755062 B1 **2016. 09. 28.**

(51) Int. Cl.: ***G06F 21/42*** *(2006.01)*
G06Q 20/40 *(2006.01)*
G06Q 20/42 *(2006.01)*
G06Q 30/06 *(2006.01)*
G07F 7/10 *(2006.01)*
H04L 29/06 *(2006.01)*

(30) Elsőbbségi adatok:
703605 P **2005. 07. 29.** **US**

(72) Feltaláló(k):
Grandcolas, Michael, Santa Monica, CA 90405 (US)
Koryakovtseva, Irina, Marlboro, NJ 07746 (US)
Vos, Jennifer, Glen Head, NY 11545 (US)
Herrig, Robert A., Garrison, NY 10524 (US)

(73) Jogosult(ak):
Citicorp Credit Services, Inc. (USA), Sioux Falls, SD 57104 (US)

(74) Képviselő:
SBGK Szabadalmi Ügyvivői Iroda, Budapest

(54) **Eljárások és rendszerek biztonságos felhasználói hitelesítésre**

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 755 062 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
28.09.2016 Bulletin 2016/39

(21) Application number: **06118042.8**

(22) Date of filing: **28.07.2006**

(51) Int Cl.:
G06F 21/42 *(2013.01)* ***G06Q 20/40*** *(2012.01)*
G06Q 20/42 *(2012.01)* ***G06Q 30/06*** *(2012.01)*
G07F 7/10 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(54) **METHODS AND SYSTEMS FOR SECURE USER AUTHENTICATION**

VERFAHREN UND SYSTEM FÜR SICHERE BENUTZERAUTHENTIFIZIERUNG

PROCÉDÉS ET SYSTÈMES DE SÉCURISATION DE L'AUTHENTIFICATION DE L'UTILISATEUR

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

(30) Priority: **29.07.2005 US 703605 P**

(43) Date of publication of application:
21.02.2007 Bulletin 2007/08

(73) Proprietor: **Citicorp Credit Services, Inc. (USA)**
Sioux Falls, SD 57104 (US)

(72) Inventors:
- **Grandcolas, Michael**
  Santa Monica, CA 90405 (US)
- **Koryakovtseva, Irina**
  Marlboro, NJ 07746 (US)
- **Vos, Jennifer**
  Glen Head, NY 11545 (US)
- **Herrig, Robert A.**
  Garrison, NY 10524 (US)

(74) Representative: **Johansson, Lars-Erik**
Hynell Patenttjänst AB
Box 138
683 23 Hagfors (SE)

(56) References cited:
WO-A1-01/11450
US-A- 6 078 908
US-A1- 2004 054 932
US-A1- 2004 249 503

EP 1 755 062 B1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the Invention

[0001] The present invention relates generally to the field of electronic commerce, and more particularly to methods and systems for secure user authentication in electronic commerce transactions.

Background of the Invention

[0002] Currently, credential theft is a substantial danger in the online world, for example, through "phishing", key loggers, spyware, and man-in-the middle attacks, among others. There is presently a push from both regulators and financial institutions, such as banks, to come up with two-factor authentication techniques by which the threat of a simple credential theft, such as theft of a password, is mitigated, for example, by the fact that there is some factor other than a simple password involved in authentication. A number of forms of two-factor identification have been proposed which utilize something else besides a standard password, such as a user's fingerprint, or in a physical world, a user's ATM card.

[0003] Another example of the use of something else besides a standard password is what are referred to as one-time passwords, and specifically one-time password tokens or key fobs. These one-time password tokens represent a type of standard but very expensive way to provide a customer with a device that continuously generates a time-based, or event based, one-time password. Thus, when a user prepares to log in, the user consults the device, and the device displays, for example, a number that the user keys in and which can be used only once. Thus, if an unauthorized person intercepts the particular number, it is too late for the unauthorized person to use it.

[0004] However, those types of solutions are extremely expensive and are not necessarily user friendly. For example, customers are typically required to carry their tokens around with them, and if a customer has relationships, for example, with three or four banks, the customer is required to carry around three or four different tokens. In addition, the tokens have a limited useful life after which they must be replaced. Further, the task of distributing the tokens to users creates issues of security and expense for financial institutions, and security and convenience issues are likewise created on the customer's side in keeping up with their multiple tokens.

[0005] A particularly troublesome aspect of credential theft is electronic fraud in which increasing numbers of unsuspecting customers of financial institutions, such as banks, are phished by being sent emails attempting to trick them into revealing their user names and passwords or PINs to an unauthorized party. Typically, an unauthorized party who succeeds in capturing the log-in credentials of a bank customer through email phishing or perhaps via software viruses, reuses the customer's credentials to log on to the bank's online banking website to perform fraudulent transactions. One such type of fraudulent transaction involves use of the customer's stolen log-in credentials to move money internationally by wire transfer, and another type of fraud is a transaction referred to as a global intercity transaction that involves moving money, for example, from a bank account in the United States to a foreign bank account and withdrawing the money.

[0006] WO01/11450 discloses a security architecture in which a single sign-on is provided for multiple information resources. Authentication schemes are associated with trust levels and a log-on service obtains credentials commensurate with the trust level requirements.

Summary of the Invention

[0007] The invention is defined by the scope of the appended claims.

Brief Description of the Drawings

[0008]

Fig. 1 is a schematic diagram that illustrates an example of key components and the flow of information between key components of a secure user authentication system for embodiments of the invention;

Fig. 2 is a flow chart that illustrates an example of a next-time password aspect process for embodiments of the invention;

Fig. 3 is a flow chart that illustrates an example of the pending stage of a transaction provider enforced one-time authentication code aspect process for embodiments of the invention;

Fig. 4 is a flow chart that illustrates an example of the activation stage of the transaction provider enforced one-time authentication code aspect process for embodiments of the invention;

Fig. 5 is a flow chart that illustrates an example of the request access code stage of a navigation provider-enforced authentication code aspect process for embodiments of the invention;

Fig. 6 is a flow chart that illustrates an example of the access allowed stage of the navigation provider enforced authentication code aspect process for embodiments of the invention;

Fig. 7 is a flow chart that illustrates an example of the request access code stage of a hybrid navigation provider-enforced / transaction provider-enforced-plus-aware menus authentication code aspect process for embodiments of the invention;

Fig. 8 is a flow chart that illustrates an example of the access allowed stage of the hybrid process for embodiments of the invention;

Fig. 9 is a sample payments and transfers GUI menu screen for the secure transaction code aspect of embodiments of the invention;

Fig. 10 is a sample transfer authorization code entry GUI screen for the secure transaction code aspect of embodiments of the invention;

Fig. 11 is a sample transfer authorization code confirmation GUI screen for the secure transaction code aspect of embodiments of the invention;

Fig. 12 is a sample email address error GUI page for the secure transaction code aspect of embodiments of the invention;

Fig. 13 is a sample authorization code error GUI page for the secure transaction code aspect of embodiments of the invention;

Fig. 14 is a sample authorization code email message for the secure transaction code aspect of embodiments of the invention;

Fig. 15 is a sample change email notification message for the secure transaction code aspect of embodiments of the invention;

Fig. 16 is a sample home page displaying the customer's current email address for the secure transaction code aspect of embodiments of the invention; and

Fig. 17 is a sample home page displaying the customer's current email address with a notification of a recently changed email address for the secure transaction code aspect of embodiments of the invention.

Detailed Description

[0009] Reference will now be made in detail to embodiments of the invention, one or more examples of which are illustrated in the accompanying drawings. Each example is provided by way of explanation of the invention and not as a limitation of the invention. It will be apparent to those skilled in the art that various modifications and variations can be made in the present invention without departing from the scope of the invention. For instance, features illustrated or described as part of one embodiment can be used on another embodiment to yield a still further embodiment. Thus, it is intended that the present invention cover such modifications and variations that come within the scope of the invention.

[0010] A next-time password aspect of embodiments of the present invention proposes a different form of one-time passwords that leverages existing technology. A key to a one-time password embodiment is that it is given to a user on some channel that is outside the manner in which the user accesses, for example, the user's Internet service. As previously noted, current one-time password solutions require the user to carry a separate device which generates a time-based, one-time password. These devices are expensive and inconvenient, and they take up space, for example, on a key chain. However, almost everyone has a cell phone or email address, and cell phone usage is growing. In an embodiment of the invention, every time a user, such as a financial institution customer, logs off of the financial institution's site, a next-time-password is sent to the customer's pre-registered delivery address, such as the customer's cell phone or email address or other out-of-band channel, by the financial institution, for example, via text message.

[0011] The next-time password for an embodiment of the invention is good for one-time use and optionally can also have an expiry time and/or date associated with it, after which the next-time password is no longer valid. It is to be understood that while the present example refers to sending the next-time password to a cell phone, a mobile phone or an email address, the channel for delivery of the next-time password can be any other suitable communication channel, such as some type of e-mail account or even a voice mail to the customer's home phone, that is out of band or different from the communication channel by which the customer communicates with the institution's site. Thereafter, when the customer returns to the financial institution's site, the customer can enter the customer's normal login credentials, such as the customer's username and password. In addition, the customer can consult, for example, the customer's cell phone and find the next-time password which was stored in the customer's cell phone under saved messages.

[0012] In the next-time password aspect of embodiments of the invention, if for some reason the customer does not have a next-time password or is unable to find the next-time password stored in the customer's mobile phone, it is only necessary for the customer to enter his or her username and password to be allowed into the financial institution's site. At the same time the customer comes into the site, a next-time password is immediately sent to the customer's registered cell phone or other delivery device. Then, upon receiving the next-time password in real time or pseudo-real time, the customer can enter the next-time password and be allowed full access into the entire site.

[0013] The next-time password solution for embodiments of the invention does not require any phone resident software to generate a next-time password token. While it can be argued that a constantly changing token value may be slightly safer than the next-time password, since the next-time password is unique to the customer and can be used only once, the realistic chance of the

next-time password being intercepted is extremely low, and it provides a very effective one-time password. Moreover, a financial institution may typically have most of the infrastructure in place to implement the next-time password for embodiments of the invention.

[0014] For an example of use of the next-time password for embodiments of the invention, a customer at a computing device with a browser logs onto a financial institution's online banking website by entering his or her username and password. In addition, the customer locates his or her next-time password among saved messages on the customer's mobile phone and enters the next-time password. The next-time password is valid for only one use and as soon as the customer enters the next-time password, it is no longer valid for any purpose. Thereafter, when the customer logs off, another next-time password is sent to the customer's registered communication device, such as the customer's mobile phone. Thus, even if an unauthorized party intercepts the customer's next-time password, any interception will most likely occur after the next-time password has already been used. In other words, if the next-time password is intercepted via a key logger, is it too late, because the next-time password was already used when the customer entered the financial institution's site and is no longer valid for any purpose.

[0015] Accordingly, the next-time password for embodiments of the invention has all the characteristics of a one-time password except that instead of constantly being generated, for example, every few seconds, the next-time password is sent to the customer when he or she logs out of a site for use when the customer returns to the site at a later time. Further, if the customer is unable to find his or her next-time password when he or she wants to return to the financial institution's site, the customer simply enters his or her username and password and then, for example, clicks on a button to say that he or she does not have his or her next-time password. In response, the financial institution immediately sends a next-time password to the customer's registered device, which the customer can then enter for full access to the site, for example, for online banking.

[0016] Fig. 1 is a schematic diagram that illustrates an example of key components and the flow of information between key components of a secure user authentication system for embodiments of the invention. Referring to Fig. 1, the system for embodiments of the invention includes, for example, a customer's computing device 10, such as the customer's PC, laptop, or PDA, is coupled over a network 12, such as the Internet or other global network, to a portal server 12 by which a user, such as a customer, accesses a web site. The portal server 12 can be the portal server of any entity, including for example, a financial institution, such as a bank. In addition, an alert message server 16 provides, for example, email messages to the customer at the customer's computing device 10 via the network 12 or the message server 16 can provide, for example, text messages to the customer's telecommunication device 18, such as a mobile or land phone, via a telecommunication system 20. Further, the portal server 14 may also provide access to one or more transaction servers 22, which can include a federation of such servers.

[0017] Fig. 2 is a flow chart that illustrates an example of a next-time password aspect process for embodiments of the invention. Referring to Fig. 2, at S1, each time the customer logs off, for example, the financial institution's web site 14, a next-time password unique to the customer that can be used only once (and optionally can have an expiry time and/or date) is sent to the customer via an out-of-band communication channel, such as to the customer's pre-registered email address or cell phone 18 by the financial institution, for example, via text message. At S2, when the customer returns to the web site 14 on a succeeding occasion, the customer logs on by entering the customer's normal login credentials, such as the customer's username and password, and in addition, the customer consults, for example, the stored messages on the customer's cell phone 18 or email on the customer's computing device 10 to find the next-time password which was received when the customer logged off the web site 14 on the preceding occasion and stored in the customer's cell phone under saved messages or in the customer's email folder, and the customer enters the next-time password for full access to the entire site.

[0018] Referring again to Fig. 2, at S3, if for some reason the customer does not have or is unable to find the stored or saved next-time password, the customer can enter his or her username and password and is allowed to log on to the financial institution's site 14, and at the same or substantially the same time that the customer logs onto the site, a next-time password is immediately sent out-of-band to the customer's registered cell phone 18 or other device, and upon receiving the next-time password, the customer can enter the next-time password and be allowed full access into the entire site. Thereafter, at S4, when the customer logs off, another next-time password is sent out-of-band to the customer's registered communication device, such as the customer's mobile phone 18.

[0019] While the foregoing example refers to accessing an online financial institution or banking web site, use of the next-time password for embodiments of the invention is in no way limited to the site of a bank or other type of financial institution. Nor is use of the next-time password limited to accessing a web site. For example, the next-time password can also be employed in an automatic teller machine (ATM) system, as well as in any other operation in which a customer is required to enter authentication information. In addition, while as previously mentioned, the next-time password solution for embodiments of the invention does not require phone-resident software to generate the next-time password, alternative embodiments of the invention involve, for example, providing the customer a simple phone-resident application that makes it easier and more convenient for

the customer to save and view the next-time password token that was sent to his or her cell phone 18. Another alternative aspect for embodiments of the invention involves, for example, a phone-resident application that generates the next-time password token.

[0020] A key feature of the next-time password aspect for embodiments of the invention is that every time a customer logs off the financial institution's site 14, a next-time password is sent to the customer's registered device, such as the customer's cell phone 18, and the next time the customer logs on, in addition to entering his or her username and password, the customer simply consults messages store on his or her mobile phone 18, which is typically in the customer's immediate possession, and finds and enters the previously provided next-time password. Thus, the customer is not required to carry anything that he or she does not typically carry anyway.

[0021] It is to be understood that while the next-time password solution for embodiments of the invention can be implemented by any number of different types of entities, including without limitation, financial institutions, such as banks, as well as other types of financial institutions, the usefulness of the next-time password is not limited to financial institutions, and it can be implemented for logging into other types of sites as well. The next-time password aspect of embodiments of the invention combines elements to provide a one-time password in the form of the next-time password that, while it does not constantly change, changes often enough and is delivered in a way that is secure enough that the chances of interception and theft, especially mass theft, are extremely low. Further, the implementation and use of the next-time password solution for embodiments of the invention is extremely economical and does not require the purchase and distribution of expensive token devices. Nor is it dependent on different versions of phones and will work with virtually any phone that supports, for example, text messaging.

[0022] The secure transaction code aspect for embodiments of the invention provides an approach to protect a bank's customers from fraudulent transactions even if their primary log-in credentials are stolen. In the secure transaction code aspect, the procedure in which a customer uses the customer's log-in credentials to log on to the bank's system remains unchanged, but if the customer attempts to perform certain pre-defined types of transactions deemed by the bank to be sensitive functions, such as wire transfers or global intercity transfers, the customer must answer a one-time value, i.e., the secure transaction code, in order to execute the sensitive transaction. In the secure transaction code aspect, the one-time value that is the secure transaction code is likewise sent to the customer out of band of the Internet channel to the customer's pre-registered delivery address, such as the customer's email address or cell phone 18. As in the next-time password aspect, the customer must have previously registered a delivery destination address, as an email address or a cell phone number as the delivery vehicle for the customer's secure transaction code. Upon receipt by the customer of the secure transaction code at the customer's email address or cell phone 18, the customer views the value and answers it on the website 12 and is then allowed to proceed and execute the transaction deemed by the bank to be a sensitive function.

[0023] A feature of the secure transaction code aspect for embodiments of the invention relates to a further manner of protecting access inside the bank's website. Because there are potentially a multitude of different kinds of functions that can be protected by the secure transaction code, an embodiment of the invention deploys the main gating protection in the navigation of the site itself. Thus, when a customer tries to click on a function or a navigation link that would take the customer to a sensitive function, the customer is requested to enter a secure transaction code. If the customer who is asked to enter a secure transaction code does not have one, the customer can respond via the GUI of the website 12 that he or she does not have a secure transaction code. Thereupon, the navigational aspect of the site 12 working with a security component of the site 12 generates a secure transaction code and causes it to be delivered, for example, to the customer's email address or cell phone 18. Upon receipt of the secure transaction code, even within the same session, the customer can enter the value representing the secure transaction code and is allowed to proceed.

[0024] A further feature of the secure transaction code aspect of embodiments of the invention relates to providing protection for functions that are both on the bank's primary site 14 itself and on any of a number of federated sites that are also part of the bank's online banking functionality, including for example, sites for a functionality that is the executor for global intercity transfers and a functionality that is the executing system for wire transfers. Providing this protection involves, for example, tasking an indicator for a single sign-on mechanism of the bank to the federated sites 22 telling the federated sites 22 that the customer has requested a secure function and advising the federated sites 22 whether or not the customer has entered a secure transaction code.

[0025] The secure transaction code aspect for embodiments of the invention is viewed as a form of a one-time password, meaning that it can be entered only once, and once it has been entered, it can never be used again. Thus, if the secure transaction code is stolen, it has no value. The secure transaction code can also have a time period for which it remains valid, which can any suitable length of time, such as a few minutes up to several days. Thus, when a secure transaction code is issued, the customer is notified that it is valid for only the pre-determined amount of time, after which it expires. However, the customer is also made aware that he or she can receive a new secure transaction code in advance of the next occasion on which he or she may want to perform one of the sensitive functions, and the secure transaction code

can also be used for performing multiple sensitive transactions within a single customer session once the customer enters the secure transaction code.

[0026] Referring to Fig. 1, in an example of the secure transaction code aspect for embodiments of the invention, when the customer selects a link on a financial institution portal 14 to a sensitive transaction, an authorization page is displayed that explains the need for an authorization code to access the particular function. For example, when the customer clicks on a link for a function deemed by the financial institution to be a sensitive transaction, such as wire transfer, within a menu page, the link brings up the authorization page. If the financial institution portal 14 detects that the customer does not have an email address on the customer's stored profile, a modified version of the authorization page is brought up. The portal 14 confirms whether or not the customer is entitled to the wire transfer functionality and if so, the portal 14 retrieves the customer's pre-registered email address and the date when it was last modified on the customer's stored profile record. The portal 14 causes a random secret code (i.e., secure transaction code) to be issued for the customer and stored on the customer's profile record, as well as the secret code issue date. In addition, the portal 14 causes an email to be sent out-of-band to the customer with the secret code. Upon entry of the secret code by the customer on the authorization page, the secret code entered by the customer is compared by the portal 14 with the stored secret code and its expiration date.

[0027] In embodiments of the secure transaction code aspect of the invention, alerts are sent to customers whenever the email address on the customer's profile is changed. For example, the portal 14 can send one or more messages to the customer via postal service about the changed email address. In addition, the current customer profile e-mail address can be displayed on the customer's signed-on home page, along with a link to edit the address. Further, whenever an email address change is made, a notification that the address has been changed can be displayed on the customer's signed-on home page. If the customer enters the secret code after it has expired, a message is displayed advising the customer to request a new secret code and the customer is routed to a new code request screen. If the code is entered correctly and has not expired, the customer is routed to the appropriate screen for the requested sensitive transaction. If the code entered is incorrect, an error screen is displayed and an attempt counter is increased.

[0028] Embodiments of the secure transaction code aspect provide, for example, a transaction provider-enforced one-time authentication code process with a pending stage and an activation stage; a navigation provider-enforced authentication code process with a request access code stage and an access allowed stage; and/or a hybrid navigation provider-enforced / transaction provider-enforced-plus-aware menus authentication code process, likewise with a request access code stage and an access allowed stage. Fig. 3 is a flow chart that illustrates an example of the pending stage of the transaction provider-enforced one-time authentication code aspect process for embodiments of the invention. In the transaction provider enforced process, the transaction provider is responsible for the additional authentication enforcement and supports the pending or setup stage, as well as the activate of execute stage.

[0029] Referring to Fig. 3, at S11, the customer at a computing device 10 with a browser logs on, for example, the financial institution's home banking portal server 14 and selects a sensitive transaction task, such as a wire transfer, is redirected to a financial institution transaction server 22, enters information to set up the transaction, and is informed that a one-time activation code (i.e., secure transaction code) will be emailed to the customer. Referring further to Fig. 3, at S12, the transaction server 22 carries on a dialog with the customer to set-up the wire transfer and pends the transaction to a database. At S 13, the transaction server 22 generates, stores, and sends the one-time activation code to a financial institution alert message server 16 for delivery to the customer's email address. At S14, the alert message server 16 sends the one-time code to the customer's email address if the email address has not recently changed. At S15, the customer at the customer's computing device 10 receives the email with the one-time code.

[0030] Fig. 4 is a flow chart that illustrates an example of the activation stage of the transaction provider enforced one-time authentication code aspect process for embodiments of the invention. Referring to Fig. 4, at S16, the customer at the computing device 10 with the browser logs on the financial institution's home banking portal server 14, enters a selection for the sensitive transaction task, is redirected to the transaction server 22, and enters the one-time code when prompted by the transaction server 22. At S17, the transaction server determines whether or not the one-time code is valid, and if valid, activates the transaction and sends a response confirming activation of the transaction to the customer.

[0031] Fig. 5 is a flow chart that illustrates an example of the request access code stage of the navigation provider enforced authentication code aspect for embodiments of the invention. In the navigation provider enforced process, the navigation provider provides enforcement on a navigation task basis in which, for example, a customer is not allowed to enter a navigation task without an authentication access code. It is to be understood that the authentication access code can be any one of a one-time use code, or a multi-use code with an expiration time or date, or use-count code. Referring to Fig. 5, at S21, the customer at the computing device 10 with a browser logs on the financial institution's home banking portal server 14 and selects a sensitive transaction task, such as a wire transfer, is prompted by the portal server 14 to enter the customer's authentication access code (i.e., secure access code), and if the customer responds that her or she does not have an authentication access code,

is informed by the portal server 14 that an authentication access code will be emailed to the customer. At S22, the portal server 14 generates an access code for the customer's use for the particular sensitive transaction and sends the access to the customer's email address via a financial institution alert message server 16. At S23, the alert message server 16 sends the access code to the customer's email address if the email address has not recently changed. At S24, the customer at the customer's computing device 10 receives the email with the one-time code.

[0032] Fig. 6 is a flow chart that illustrates an example of the access allowed stage of the navigation provider-enforced authentication code aspect process for embodiments of the invention. Referring to Fig. 6, at S25, the customer at the computing device 10 with the browser logs on the financial institution's home banking portal server 14, enters a selection for the sensitive transaction task, and enters the access code. At S26, the portal server 14 determines whether or not the access code is valid for the particular task, and if valid, allows entry to the task, for example, by redirecting the customer's browser to the transaction server 22. It is noted that in the navigation provider enforced process, the transaction provider or providers are transparent to the authentication process. It is to be further noted that the customer can perform more that one sensitive transaction during a session and there is no need to pend transactions.

[0033] Fig. 7 is a flow chart that illustrates an example of the request access code stage of the hybrid navigation provider-enforced / transaction provider-enforced-plus-aware menus authentication code aspect process for embodiments of the invention. In the hybrid process, the navigation provider likewise provides enforcement on a navigation task basis in which, for example, a customer is not allowed to enter a navigation task without an authentication access code (i.e., secure access code). It is likewise to be understood that the authentication access code can be any one of a one-time use code, or a multi-use code with an expiration time or date, or use-count code. Referring to Fig. 7, at S31, the customer at a computing device 10 with a browser logs on the financial institution's home banking portal server 14 and selects a sensitive transaction task, such as a wire transfer, is prompted by the portal server 14 to enter the customer's authentication access code, and if the customer responds that her or she does not have an authentication access code, is informed by the portal server 14 that an authentication access code will be emailed to the customer. At S32, the portal server 14 generates an access code for the customer's use for the particular sensitive transaction and sends the access code to the customer's email address via a financial institution alert message server 16. At S33, the alert message server 16 sends the access code to the customer's email address if the email address has not recently changed. At S34, the customer at the customer's computing device 10 receives the email with the one-time code.

[0034] Fig. 8 is a flow chart that illustrates an example of the access allowed stage of the hybrid process for embodiments of the invention. Referring to Fig. 8, at S35, the customer at the computing device 10 with the browser logs on the financial institution's home banking portal server 14, enters a selection for the sensitive transaction task, and enters the access code. At S26, the portal server 14 determines whether or not the access code is valid for the particular talk, and if valid, allows entry to the task, for example, by redirecting the customer's browser to the transaction server 22 with a flag indicating that the customer is entitled for sensitive transactions, in which case the customer is allowed to perform all transactions. Otherwise, without the entitlement flag, the customer is allowed to perform only non-sensitive transactions. It is noted that in the hybrid process, the transaction provider or providers are transparent to the authentication process. It is to be further noted that the customer can perform more that one sensitive transaction during a session and there is no need to pend transactions.

[0035] The secure transaction code for embodiments of the invention provides an additional level of protection for highly sensitive transactions, such as wire transfers or other high-risk transactions, by requiring a customer to use a transaction authorization code (i.e., secure access code) to make each such transaction. Thus, when a customer selects a link to a sensitive transaction, an authorization page is displayed to the customer explaining the need for an authorization code to access the function. The page also presents options for the customer to enter a code, to request a code, or to access a non-sensitive function. Customers who already possess a code can exercise the first option and enter a code in an entry field. Customers who do not already possess a code can exercise the second option to request a code and be sent a randomly generated code via e-mail using the customer's email address in the user profile. The signed-on customer in the same or a later session then provides the transaction code to authorize the requested sensitive function or possibly to authorize some other sensitive function. The transaction code expires a pre-determined time after issuance, such as one week.

[0036] In embodiments of the invention, whenever a customer changes the customer's profile e-mail address, a flag is set on the stored profile prohibiting the sending of a transaction code to the customer at the customer's email address. The flag can also be set to expire after a pre-determined period, such as one week. During that period of time, if the customer requests that he or she be sent a transaction code via e-mail, an error page is presented advising the customer that a transaction code cannot be sent, and that if the customer needs to perform a sensitive transaction, such as a wire transfer in the meantime, the transaction can be performed in person at a financial institution office. Alternatively, the error page can direct the customer to call a number for customer service, for example, for manual authentication by a customer service representative. Upon manually au-

thenticating the customer, the customer service representative can provide a random transaction code for the customer or clear the e-mail flag, whereupon the customer can request the code online and receive it at the customer's new e-mail address. Customers who exercise the third option to access non-sensitive functions are provided information only. For example, in the case of wire transfers, the customer is presented a menu with options to view information about wire transfers that are planned, past, or incoming.

[0037] In embodiments of the invention, whenever the e-mail address in the customer's stored user profile is changed, an alert is sent by email to both the new email address and to the changed email address. Further, the customer's current user profile e-mail address is displayed on the customer's signed-on home page, along with a link to edit the address. In addition, whenever an email address change is made, a notification is displayed for the customer that the email address has been changed.

[0038] Embodiments of the invention employ various GUI screens. It is to be understood that while the example flow and screens described herein relate to sensitive transactions, such as wire transfers, the same transaction authentication process for embodiments of the invention is equally useful and easily portable to other sensitive transaction types. Fig. 9 is a sample payments and transfers GUI menu screen 40 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 9, if a customer selects a sensitive function, such as "Transfer to an Account in the U.S." 42 or "Transfer to an Account Abroad" 44, a link brings up a transaction authorization entry screen.

[0039] Fig. 10 is a sample transfer authorization code entry GUI screen 46 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 10, the customer is presented with options of requesting an authorization code 48, entering an authorization code previously provided to the customer 50, or selecting a non-sensitive (informational) function 52. If the customer enters a transaction authorization code and the authorization code is authenticated, an appropriate sensitive transaction menu is presented for the customer. If the authorization code is not authenticated, an authorization code error screen is displayed for the customer. In addition, the customer can select "Cancel" 54 and return to the payments and transfers menu 40. Referring further to Fig. 10, if the customer enters a selection requesting that a code be sent to the customer 48, if no authorization flag is set on the customer's profile email address, a transfer authorization code confirmation GUI screen is displayed for the customer. However, if an authorization flag is set on the customer's profile email address, an error page is displayed informing the customer that the code cannot be sent by email. An update address link 56 allows the customer to update the customer's email address. If the customer enters a selection to see information about recent activity 52, the customer is offered further options to view information about planned wire transfers, past wire transfers, and incoming wire transfers

[0040] Fig. 11 is a sample transfer authorization code confirmation GUI screen 58 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 11, the transfer authorization code confirmation GUI page 58 notifies the customer that a code has been sent and advises the customer how to use the transfer authorization code. When the customer clicks on "Continue" 60, the customer is returned to the transfer authorization code entry screen 40. Fig. 12 is a sample email address error GUI page 62 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 12, when the customer has changed the customer's profile e-mail address within a pre-determined preceding period of time, such as in the past week, the error page 62 is presented to the customer to advise the customer of the situation. Fig. 13 is a sample authorization code error GUI page 64 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 13, when an authorization code is not authorized by the system, an "Information Not Recognized" error message 66 is presented for the customer on the authorization code error page 64. After a pre-determined number of unsuccessful attempts, such as three such attempts, to match the authorization code, the customer's personal identification number, such as a PIN or CIN, is blocked.

[0041] Fig. 14 is a sample authorization code email message 68 for the secure transaction code aspect of embodiments of the invention. When a customer requests an authorization code, an e-mail similar to the sample email message 68 illustrated in Fig. 14 is sent to the email address associated with the customer's user profile. Fig. 15 is a sample change email notification message 70 for the secure transaction code aspect of embodiments of the invention. When a customer changes the customer's user profile email address, an e-mail similar to the sample email message 70 illustrated in Fig. 15 is sent to both the new email address according to the customer's user profile and to the old email address according to the customer's user profile.

[0042] Fig. 16 is a sample home page 72 displaying the customer's current email address 74 for the secure transaction code aspect of embodiments of the invention. Referring to Fig. 16, the customer's home page 72 displays the customer's current e-mail address 74 and also provides a link to an edit function 76 to update the customer's email address on the customer's user profile. In addition, email address changes are highlighted on the home page 72 displaying the customer's email address for a pre-determined period, such as one week. Fig. 17 is a sample home page 72 displaying the customer's current email address with a notification of a recently changed email address 78 for the secure transaction code aspect of embodiments of the invention.

[0043] A unique feature of the secure transaction code aspect for embodiments of the invention is that, unlike most one-time password mechanisms, there is no re-

quirement for the customer to have any kind of physical device that generates a unique one-time value. Instead, in the secure transaction code aspect, the bank on the server side generates the value and communicates it to the customer out of band, and upon receipt by the customer, it is only necessary for the customer to enter the value. Thus, the secure transaction code achieves secure aspects of a one-time password without the expense, inconvenience, and complications of using one-time password key fobs or similar types of one-time password generating devices.

Claims

1. A computer-implemented method for secure user authentication in electronic commerce, comprising:

   maintaining electronic information having a first aspect and a second aspect, said first aspect being accessible by a user over a first electronic communication channel in response to entry of a first credential known to the user and said second aspect being accessible by the user over the first electronic communication channel in response to entry of a second credential provided to the user;
   pre-registering a delivery address on a second electronic communication channel that is different from the first electronic communication channel for providing the second credential to the user;
   allowing a user a current session of access to the first aspect of the electronic information in response to entry of the first credential and providing the second credential to the user at the pre-registered delivery address via the second electronic communication channel in response to entry of a pre-determined user selection during said session of user access to the first aspect, wherein a change in the user's delivery address on said second electronic communication channel results in that a flag is set on a stored profile prohibiting providing of the second credential to the user, wherein said flag is set to expire after a pre-determined period of time, and allowing the user a session of access to the second aspect of the electronic information via the first electronic communication channel in response to entry of the second credential during one of said current session of user access to the first aspect and a succeeding session of user access to the first aspect.

2. The method of claim 1, wherein said first aspect further comprises pre-selected non-sensitive transaction aspects of the electronic information and said second aspect further comprises pre-selected sensitive transaction aspects of the electronic information.

3. The method of claim 1, wherein said first electronic communication channel further comprises a computing device coupled over a global network to a website server.

4. The method of claim 3, wherein said first electronic communication channel further comprises the computing device coupled over the global network to a transaction server via the website server.

5. The method of claim 1, wherein said first electronic communication channel further comprises a self-service financial transaction terminal coupled over a self-service financial transaction terminal network to a host server.

6. The method of claim 1, wherein said first credential further comprises a password selected by the user for identifying the user.

7. The method of claim 1, wherein said second credential further comprises a randomly generated secret code for identifying the user that is provided to the user.

8. The method of claim 1, wherein said second credential is provided to the user for a single session of access to the second aspect of the electronic information.

9. The method of claim 1, wherein said second credential has a pre-determined expiry, after which the second identifying credential is no longer valid for accessing the second aspect of the electronic information.

10. The method of claim 1, wherein pre-registering said delivery address on the second electronic communication channel further comprises pre-registering one of a mobile telecommunication device address and an email address for providing the user the second credential.

11. The method of claim 1, wherein providing said second credential to the user via the second electronic communication channel further comprises providing the second credential to the user by text message.

12. The method of claim 1, wherein providing said second credential to the user in response to the user selection further comprises providing the second identifying credential to the user in response to a user log-off of at a conclusion of said current session of user access to the first aspect.

13. The method of claim 12, wherein providing said second credential to the user in response to the user log-off further comprises providing the second credential to the user for use during a succeeding session of user access to the first aspect.

14. The method of claim 1, wherein providing said second credential to the user in response to the user selection further comprises providing the second credential to the user in response to a user request for the second credential during said current session of user access to the first aspect.

15. The method of claim 1, wherein providing said second credential to the user in response to the user selection further comprises providing the second credential to the user in response to a user attempt to access the second aspect of the electronic information during said current session of user access to the first aspect.

16. The method of claim 15, wherein providing said second credential to the user in response to the user attempt to access the second aspect of the electronic information further comprises providing the second credential to the user in response to a user attempt to access pre-selected sensitive transaction aspects of the electronic information.

17. The method of claim 16, wherein providing said second credential to the user in response to the user attempt to access pre-selected sensitive transaction aspects of the electronic information further comprises providing the second credential to the user in response to receiving an indication of the user's attempt to navigate to the pre-selected sensitive transaction aspects of the electronic information.

18. A computer system for secure user authentication in electronic commerce, comprising:

data storage means storing electronic information having a first aspect and a second aspect;
first electronic communication channel means over which said first aspect is accessible by a user in response to entry of a first credential known to a user and over which said second aspect is accessible by the user in response to entry of a second credential provided to the user;
second electronic communication channel means that is different from the first electronic communication channel means for providing the second credential to the user at a pre-registered delivery address;
said first electronic communication channel means being adapted for allowing the user a current session of access to the first aspect of the electronic information in response to entry of the first credential and for providing the second credential to the user at the pre-registered delivery address via the second electronic communication channel in response to entry of a pre-determined user selection during said session of user access to the first aspect wherein a change in the user's delivery address on said second electronic communication channel results in that a flag is set on a stored profile prohibiting
providing of the second credential to the user, wherein said flag is set to expire after a pre-determined period of time, and said first electronic communication channel means being further adapted for allowing the user a session of access to the second aspect of the electronic information via the first electronic communication channel in response to entry of the second credential during one of said current session of user access to the first aspect and a succeeding session of user access to the first aspect.

Patentansprüche

1. Computerimplementiertes Verfahren zur sicheren Benutzerauthentifizierung im elektronischen Handel, umfassend:

Aufrechterhalten elektronischer Informationen, die einen ersten Aspekt und einen zweiten Aspekt aufweisen, wobei auf den ersten Aspekt durch einen Benutzer über einen ersten elektronischen Kommunikationskanal zugegriffen werden kann, als Antwort auf die Eingabe einer dem Benutzer bekannten ersten Anmeldeinformation, und wobei auf den zweiten Aspekt durch den Benutzer über den ersten elektronischen Kommunikationskanal zugegriffen werden kann, als Antwort auf die Eingabe einer dem Benutzer zur Verfügung gestellten zweiten Anmeldeinformation; Vorabregistrieren einer Zusendeadresse auf einem zweiten elektronischen Kommunikationskanal, der sich von dem ersten Kommunikationskanal unterscheidet, um dem Benutzer die zweite Anmeldeinformation zur Verfügung zu stellen;
einem Benutzer eine momentane Zugriffssitzung auf den ersten Aspekt der elektronischen Informationen gewähren, als Antwort auf die Eingabe der ersten Anmeldeinformation, und dem Benutzer an der vorabregistrierten Zusendeadresse mittels des zweiten elektronischen Kommunikationskanals die zweite Anmeldeinformation zur Verfügung stellen, als Antwort auf die Eingabe einer vorbestimmten Benutzerauswahl während der Benutzerzugriffssitzung auf den ersten Aspekt, wobei eine Änderung der Zusendeadresse des Benutzers auf dem zweiten

elektronischen Kommunikationskanal darin resultiert, dass ein Flag an einem gespeicherten Profil gesetzt wird, das ein zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer verhindert, wobei das Flag gesetzt ist, um nach einer vorbestimmten Zeitperiode abzulaufen, und dem Benutzer mittels des ersten elektronischen Kommunikationskanals eine Zugriffssitzung auf den zweiten Aspekt der elektronischen Informationen gewähren, als Antwort auf die Eingabe der zweiten Anmeldeinformation während eines von der momentanen Benutzerzugriffssitzung auf den ersten Aspekt und einer nachfolgenden Benutzerzugriffssitzung auf den ersten Aspekt.

2. Verfahren nach Anspruch 1, wobei der erste Aspekt weiter vorausgewählte nicht sensible Transaktionsaspekte der elektronischen Informationen umfasst und wobei der zweite Aspekt weiter vorausgewählte sensible Transaktionsaspekte der elektronischen Informationen umfasst.

3. Verfahren nach Anspruch 1, wobei der erste elektronische Kommunikationskanal weiter eine Rechnervorrichtung umfasst, die über ein globales Netzwerk mit einem Website-Server gekoppelt ist.

4. Verfahren nach Anspruch 3, wobei der erste elektronische Kommunikationskanal weiter die Rechnervorrichtung umfasst, die über das globale Netzwerk mittels des Website-Servers mit einem Transaktions-Server gekoppelt ist.

5. Verfahren nach Anspruch 1, wobei der erste elektronische Kommunikationskanal weiter ein Selbstbedienungs-Finanztransaktionsterminal umfasst, das über ein Selbstbedienungs-Finanztransaktionsterminal-Netzwerk mit einem Hostserver gekoppelt ist.

6. Verfahren nach Anspruch 1, wobei die erste Anmeldeinformation zum Identifizieren des Benutzers weiter ein durch den Benutzer ausgewähltes Passwort umfasst.

7. Verfahren nach Anspruch 1, wobei die zweite Anmeldeinformation zum Identifizieren des Benutzers weiter einen zufällig generierten Geheimcode umfasst, welcher dem Benutzer zur Verfügung gestellt wird.

8. Verfahren nach Anspruch 1, wobei die zweite Anmeldeinformation dem Benutzer für eine einzelne Zugriffssitzung auf den zweiten Aspekt der elektronischen Informationen zur Verfügung gestellt wird.

9. Verfahren nach Anspruch 1, wobei die zweite Anmeldeinformation einen vorbestimmten Ablauf aufweist, nach welchem die zweite identifizierende Anmeldeinformation nicht länger für das Zugreifen auf den zweiten Aspekt der elektronischen Informationen gültig ist.

10. Verfahren nach Anspruch 1, wobei Vorabregistrieren der Zusendeadresse auf dem zweiten elektronischen Kommunikationskanal weiter Vorabregistrieren eines von einer Mobiltelekommunikations-Geräteadresse und einer Emailadresse zum zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer umfasst.

11. Verfahren nach Anspruch 1, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer mittels des zweiten elektronischen Kommunikationskanals weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer durch eine Textnachricht umfasst.

12. Verfahren nach Anspruch 1, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf die Benutzerauswahl weiter zur Verfügung stellen der zweiten identifizierenden Anmeldeinformation an den Benutzer umfasst, als Antwort auf ein Benutzer-Abmelden bei einer Beendigung der momentanen Benutzerzugriffssitzung auf den ersten Aspekt.

13. Verfahren nach Anspruch 12, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf das Benutzer-Abmelden weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer zur Verwendung während einer nachfolgenden Benutzerzugriffssitzung auf den ersten Aspekt umfasst.

14. Verfahren nach Anspruch 1, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf die Benutzerauswahl weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer umfasst, als Antwort auf eine Benutzeranforderung der zweiten Anmeldeinformation während der momentanen Benutzerzugriffssitzung auf den ersten Aspekt.

15. Verfahren nach Anspruch 1, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf die Benutzerauswahl weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer umfasst, als Antwort auf einen Benutzerzugriffsversuch auf den zweiten Aspekt der elektronischen Informationen während der momentanen Benutzerzugriffssitzung auf den ersten Aspekt.

16. Verfahren nach Anspruch 15, wobei zur Verfügung

stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf den Benutzerzugriffsversuch auf den zweiten Aspekt der elektronischen Informationen weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer umfasst, als Antwort auf einen Benutzerzugriffsversuch auf vorausgewählte sensible Transaktionsaspekte der elektronischen Informationen.

17. Verfahren nach Anspruch 16, wobei zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer als Antwort auf einen Benutzerzugriffsversuch auf vorausgewählte sensible Transaktionsaspekte der elektronischen Informationen weiter zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer umfasst, als Antwort auf Erhalten einer Meldung des Benutzerversuchs zu den vorausgewählten sensiblen Transaktionsaspekten der elektronischen Informationen zu navigieren.

18. Computersystem zur sicheren Benutzerauthentifizierung im elektronischen Handel, umfassend:

Datenspeichermittel, die elektronische Informationen speichern, welche einen ersten und einen zweiten Aspekt aufweisen;
ein erstes elektronisches Kommunikationskanalmittel, über welches durch einen Benutzer auf den ersten Aspekt zugegriffen werden kann, als Antwort auf die Eingabe einer einem Benutzer bekannten ersten Anmeldeinformation, und über welche durch den Benutzer auf den zweiten Aspekt zugegriffen werden kann, als Antwort auf die Eingabe einer dem Benutzer zur Verfügung gestellten zweiten Anmeldeinformation;
ein zweites elektronisches Kommunikationskanalmittel, welches sich von dem ersten elektronischen Kommunikationskanalmittel unterscheidet, zum zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer an eine vorabregistrierte Zusendeadresse;
wobei das erste elektronische Kommunikationskanalmittel angepasst ist, um dem Benutzer als Antwort auf die Eingabe der ersten Anmeldeinformation eine momentane Zugriffssitzung auf den ersten Aspekt der elektronischen Informationen zu gewähren, und das angepasst ist, um dem Benutzer mittels des zweiten elektronischen Kommunikationskanals an der vorabregistrierten Zusendeadresse die zweite Anmeldinformation zur Verfügung zu stellen, als Antwort auf die Eingabe einer vorbestimmten Benutzerauswahl während der Benutzerzugriffssitzung auf den ersten Aspekt, wobei eine Änderung der Zusendeadresse des Benutzers auf dem zweiten elektronischen Kommunikationskanal darin resultiert, dass ein Flag an einem gespeicherten Profil gesetzt wird, das ein zur Verfügung stellen der zweiten Anmeldeinformation an den Benutzer verhindert, wobei das Flag gesetzt ist, um nach einer vorbestimmten Zeitperiode abzulaufen, und wobei das erste elektronische Kommunikationskanalmittel weiter angepasst ist, um dem Benutzer mittels des ersten elektronischen Kommunikationskanals eine Zugriffssitzung auf den zweiten Aspekt der elektronischen Informationen zu gewähren, als Antwort auf die Eingabe der zweiten Anmeldeinformation während eines von der momentanen Benutzerzugriffssitzung auf den ersten Aspekt und einer nachfolgenden Benutzerzugriffssitzung auf den ersten Aspekt.

Revendications

1. Un procédé mis en oeuvre par ordinateur pour une authentification sécurisée de l'utilisateur dans le domaine du commerce électronique, comprenant :

le fait de maintenir une information électronique ayant un premier élément et un deuxième élément, ledit premier élément étant accessible à un utilisateur par un premier canal de communication électronique en réponse à l'entrée d'une première accréditation connue de l'utilisateur et ledit deuxième élément étant accessible à l'utilisateur par le premier canal de communication électronique en réponse à l'entrée d'une deuxième accréditation fournie à l'utilisateur ;
le fait de préenregistrer une adresse de fourniture sur un deuxième canal de communication électronique qui est différent du premier canal de communication électronique pour fournir la deuxième accréditation à l'utilisateur ;
le fait de permettre à un utilisateur une session d'accès au premier élément de l'information électronique en réponse à l'entrée de la première accréditation et fournir la deuxième accréditation à l'utilisateur à l'adresse de fourniture préenregistrée au moyen du deuxième canal de communication électronique en réponse à l'entrée d'une sélection d'utilisateur prédéterminée du premier élément au cours de ladite session d'accès de l'utilisateur, dans lequel un changement dans l'adresse de fourniture de l'utilisateur sur ledit deuxième canal de communication électronique se traduit par le fait qu'un drapeau est mis en place sur un profil stocké interdisant la fourniture de la deuxième accréditation à l'utilisateur, dans lequel ledit drapeau est configuré pour expirer après une période prédéterminée de temps, et autorisant à l'utilisateur une session d'accès au deuxième élément d'information électronique sur le premier canal de communication électronique en réponse à l'entrée de la

deuxième accréditation durant une parmi ladite session en cours d'accès de l'utilisateur au premier élément et une session ultérieure d'accès de l'utilisateur au premier élément.

2. Le procédé selon la revendication 1, dans lequel ledit premier élément comprend en outre des éléments de transaction non sensible présélectionnés de l'information électronique et ledit deuxième élément comprend en outre des éléments de transaction sensibles présélectionnés de l'information électronique.

3. Le procédé selon la revendication 1, dans lequel ledit premier canal de communication électronique comprend en outre un dispositif de calcul relié via un réseau global à un serveur de site Web.

4. Le procédé selon la revendication 3, dans lequel ledit premier canal de communication électronique comprend en outre le dispositif de calcul relié via le réseau global à un serveur de transaction via le serveur de site Web.

5. Le procédé selon la revendication 1, dans lequel ledit premier canal de communication électronique comprend en outre un terminal de transaction financière en libre-service relié par un réseau de terminaux de transaction financière en libre-service à un serveur hôte.

6. Le procédé selon la revendication 1, dans lequel ladite première accréditation comprend en outre un mot de passe choisi par l'utilisateur pour identifier l'utilisateur.

7. Le procédé selon la revendication 1, dans lequel ladite deuxième accréditation comprend en outre un code secret généré de manière aléatoire pour identifier l'utilisateur, qui est fourni à l'utilisateur.

8. Le procédé selon la revendication 1, dans lequel ladite deuxième accréditation est fournie à l'utilisateur pour une session unique d'accès au deuxième élément de l'information électronique.

9. Le procédé selon la revendication 1, dans lequel ladite deuxième accréditation a une échéance d'expiration prédéterminée, après laquelle la deuxième accréditation n'est plus valide pour accéder au deuxième élément de l'information électronique.

10. Le procédé selon la revendication 1, dans lequel le fait de préenregistrer ladite adresse de fourniture sur le deuxième canal de communication électronique comprend en outre le fait de préenregistrer une parmi une adresse d'un dispositif de télécommunication mobile et une adresse de courrier électronique pour fournir à l'utilisateur la deuxième accréditation.

11. Le procédé selon la revendication 1, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur via le deuxième canal de communication électronique comprend en outre le fait de fournir la deuxième accréditation à l'utilisateur par un message texte.

12. Le procédé selon la revendication 1, dans lequel le fait de fournir ladite deuxième accréditation de l'utilisateur en réponse à la sélection par l'utilisateur, comprend en outre le fait de fournir la deuxième accréditation d'identification à l'utilisateur en réponse à une déconnexion de l'utilisateur en conclusion de ladite session en cours d'accès de l'utilisateur au premier élément.

13. Le procédé selon la revendication 12, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur en réponse à une déconnexion de l'utilisateur comprend en outre le fait de fournir la deuxième accréditation à l'utilisateur pour une utilisation lors d'une session ultérieure d'accès de l'utilisateur au premier élément.

14. Le procédé selon la revendication 1, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur en réponse à la sélection par l'utilisateur comprend en outre le fait de fournir la deuxième accréditation de l'utilisateur en réponse à une demande de l'utilisateur pour la deuxième accréditation au cours de ladite session en cours d'accès de l'utilisateur au premier élément.

15. Le procédé selon la revendication 1, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur en réponse à la sélection par l'utilisateur comprend en outre le fait de fournir la deuxième accréditation à l'utilisateur en réponse à une tentative de l'utilisateur d'accéder au deuxième élément de l'information électronique au cours de ladite session en cours d'accès de l'utilisateur au premier élément.

16. Le procédé selon la revendication 15, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur en réponse à une tentative d'accès de l'utilisateur au deuxième élément de l'information électronique comprend en outre le fait de fournir la deuxième accréditation à l'utilisateur en réponse à une tentative de l'utilisateur d'accéder à des éléments de transaction sensibles présélectionnés de l'information électronique.

17. Le procédé selon la revendication 16, dans lequel le fait de fournir ladite deuxième accréditation à l'utilisateur en réponse à la tentative d'accès de l'utilisateur à des éléments de transaction sensibles présélectionnés de l'information électronique comprend en outre le fait de fournir la deuxième accréditation

à l'utilisateur en réponse à la réception d'une indication de la tentative de l'utilisateur de naviguer vers les éléments de transaction sensibles présélectionnés de l'information électronique.

18. Un système informatique pour l'authentification sécurisée de l'utilisateur dans le domaine du commerce électronique, comprenant :

un moyen de stockage de données stockant des informations électroniques comportant un premier élément et un deuxième élément ;
un premier moyen formant un canal de communication électronique par lequel ledit premier élément est accessible par un utilisateur en réponse à l'entrée d'une première accréditation connue de l'utilisateur et par lequel ledit deuxième élément est accessible par l'utilisateur en réponse à l'entrée d'une deuxième accréditation fournie à l'utilisateur ;
un deuxième moyen formant canal de communication électronique qui est différent du premier moyen de canal de communication électronique pour fournir la deuxième accréditation à l'utilisateur à une adresse de fourniture préenregistrée ;
ledit premier moyen formant canal de communication électronique étant adapté pour permettre à l'utilisateur une session courante d'accès au premier élément de l'information électronique en réponse à l'entrée de la première accréditation et pour la fourniture de la deuxième accréditation à l'utilisateur à l'adresse de fourniture préenregistrée via le deuxième canal de communication électronique en réponse à l'entrée d'une sélection de l'utilisateur prédéterminée au cours dudit accès lors de la session d'utilisateur au premier élément, dans lequel un changement d'adresse de fourniture de l'utilisateur sur ledit deuxième canal de communication électronique résulte dans le fait qu'un drapeau est installé sur un profil stocké interdisant la fourniture de la deuxième accréditation à l'utilisateur, dans lequel ledit drapeau est configuré pour expirer après une période de temps prédéterminée, et le premier moyen formant canal de communication électronique est en outre adapté pour autoriser à l'utilisateur une session d'accès au deuxième élément d'information électronique via le premier canal de communication électronique en réponse à l'entrée de la deuxième accréditation lors de l'une parmi ladite session en cours d'accès de l'utilisateur au premier élément et une session ultérieure d'accès de l'utilisateur au premier élément.

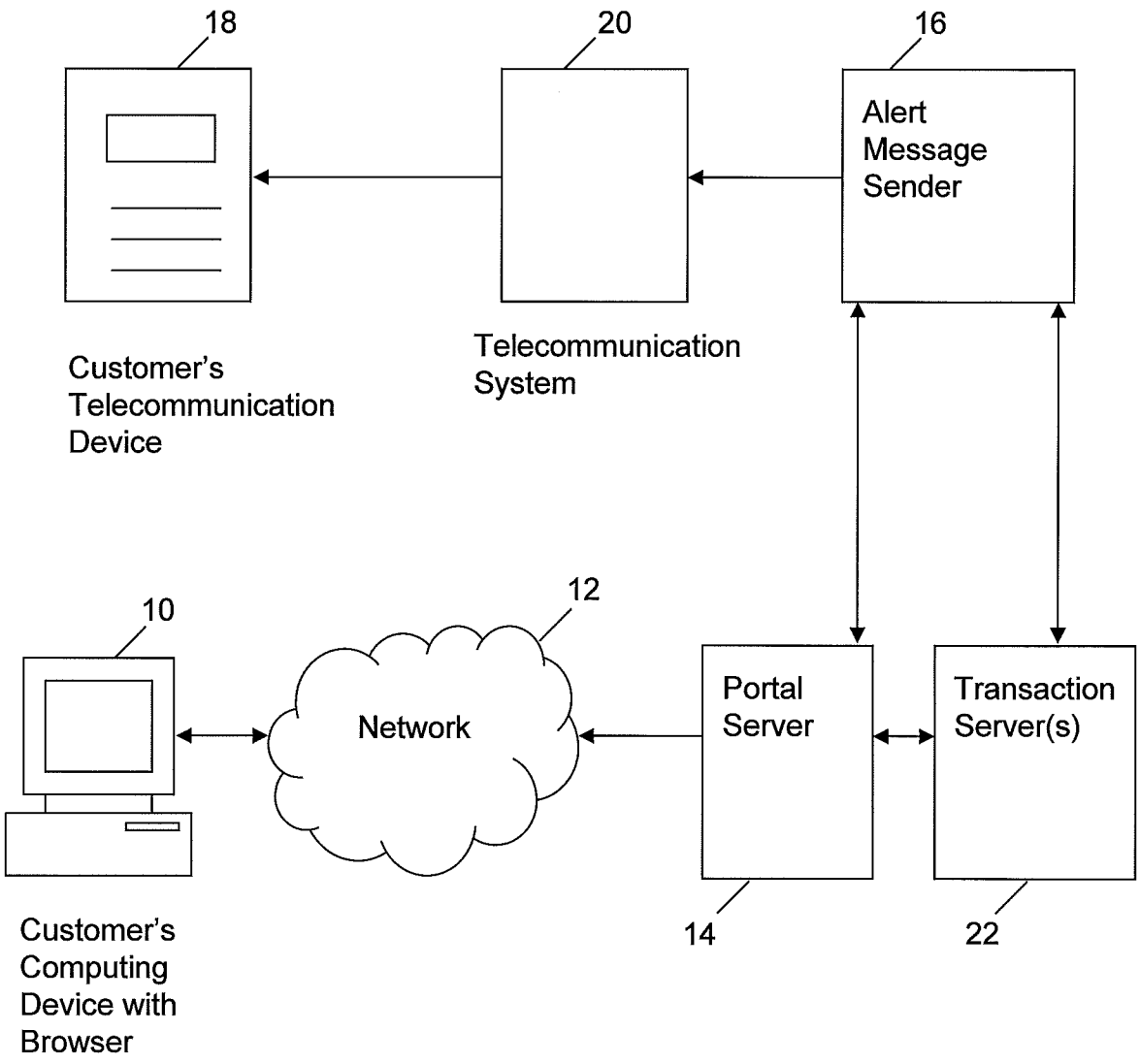
18
20
16
Alert Message Sender
Customer's Telecommunication Device
Telecommunication System
10
12
Network
Portal Server
Transaction Server(s)
Customer's Computing Device with Browser
14
22

FIG. 1

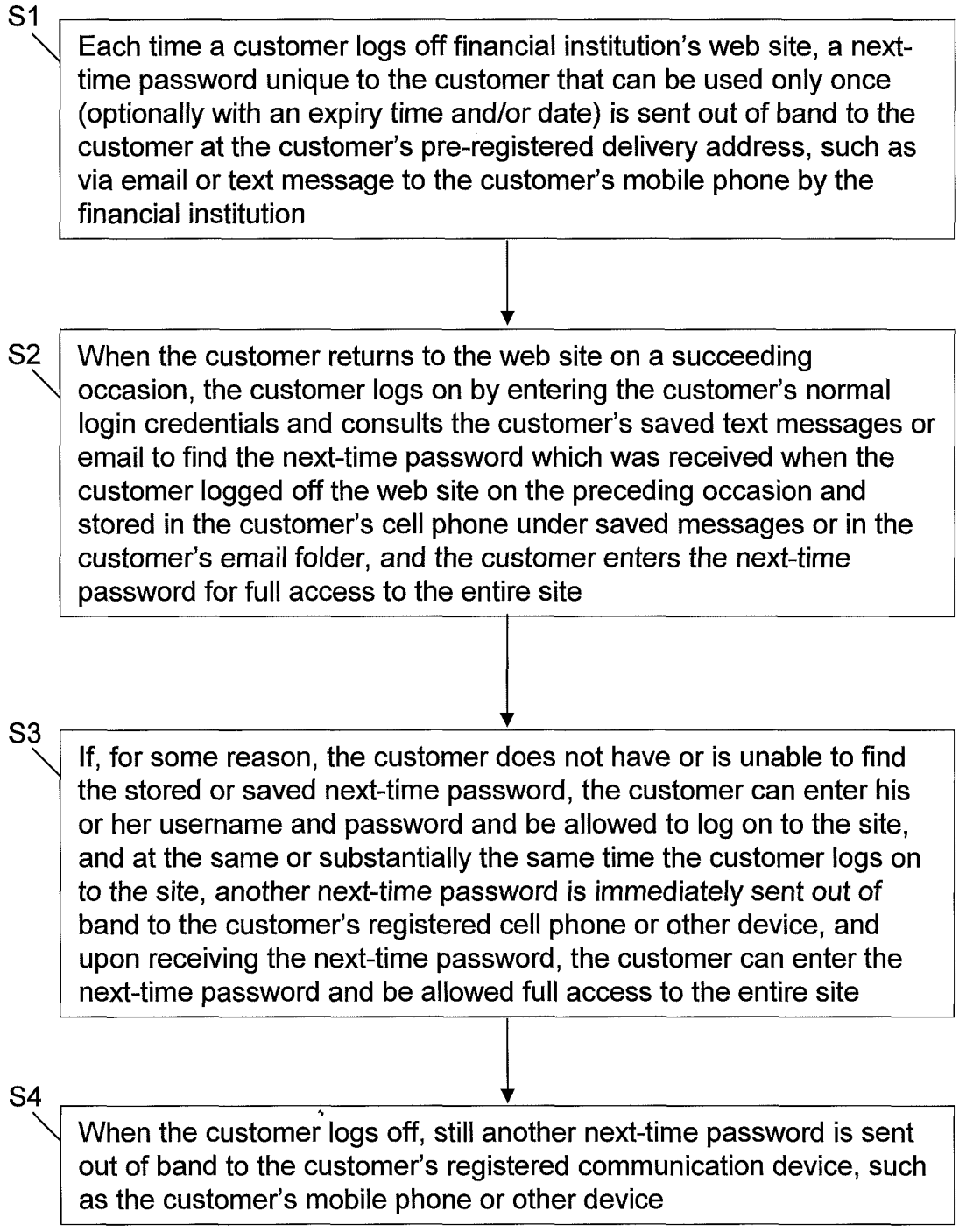
S1
Each time a customer logs off financial institution's web site, a next-time password unique to the customer that can be used only once (optionally with an expiry time and/or date) is sent out of band to the customer at the customer's pre-registered delivery address, such as via email or text message to the customer's mobile phone by the financial institution
S2
When the customer returns to the web site on a succeeding occasion, the customer logs on by entering the customer's normal login credentials and consults the customer's saved text messages or email to find the next-time password which was received when the customer logged off the web site on the preceding occasion and stored in the customer's cell phone under saved messages or in the customer's email folder, and the customer enters the next-time password for full access to the entire site
S3
If, for some reason, the customer does not have or is unable to find the stored or saved next-time password, the customer can enter his or her username and password and be allowed to log on to the site, and at the same or substantially the same time the customer logs on to the site, another next-time password is immediately sent out of band to the customer's registered cell phone or other device, and upon receiving the next-time password, the customer can enter the next-time password and be allowed full access to the entire site
S4
When the customer logs off, still another next-time password is sent out of band to the customer's registered communication device, such as the customer's mobile phone or other device

FIG. 2

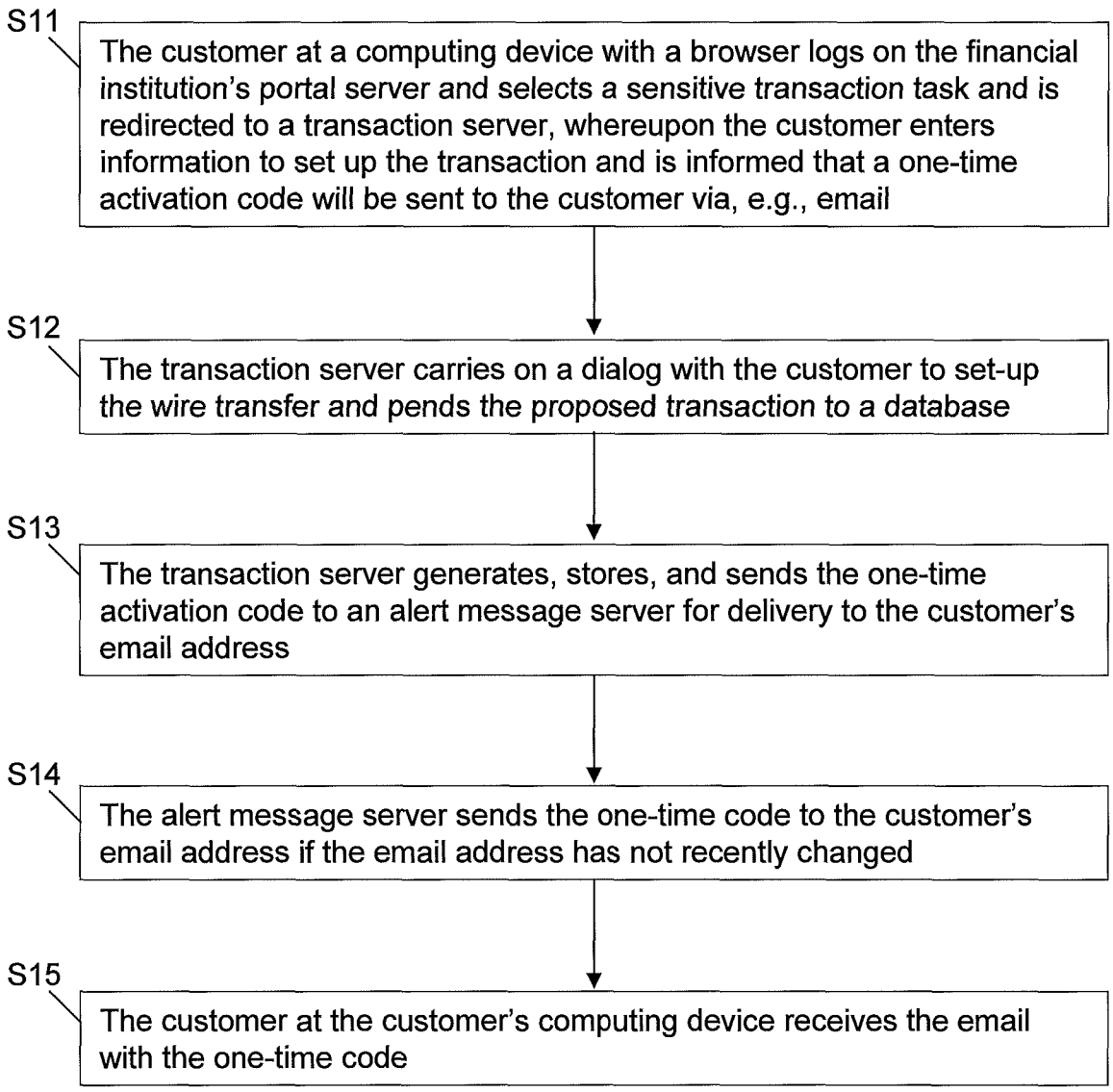
S11
The customer at a computing device with a browser logs on the financial institution's portal server and selects a sensitive transaction task and is redirected to a transaction server, whereupon the customer enters information to set up the transaction and is informed that a one-time activation code will be sent to the customer via, e.g., email
S12
The transaction server carries on a dialog with the customer to set-up the wire transfer and pends the proposed transaction to a database
S13
The transaction server generates, stores, and sends the one-time activation code to an alert message server for delivery to the customer's email address
S14
The alert message server sends the one-time code to the customer's email address if the email address has not recently changed
S15
The customer at the customer's computing device receives the email with the one-time code

FIG. 3

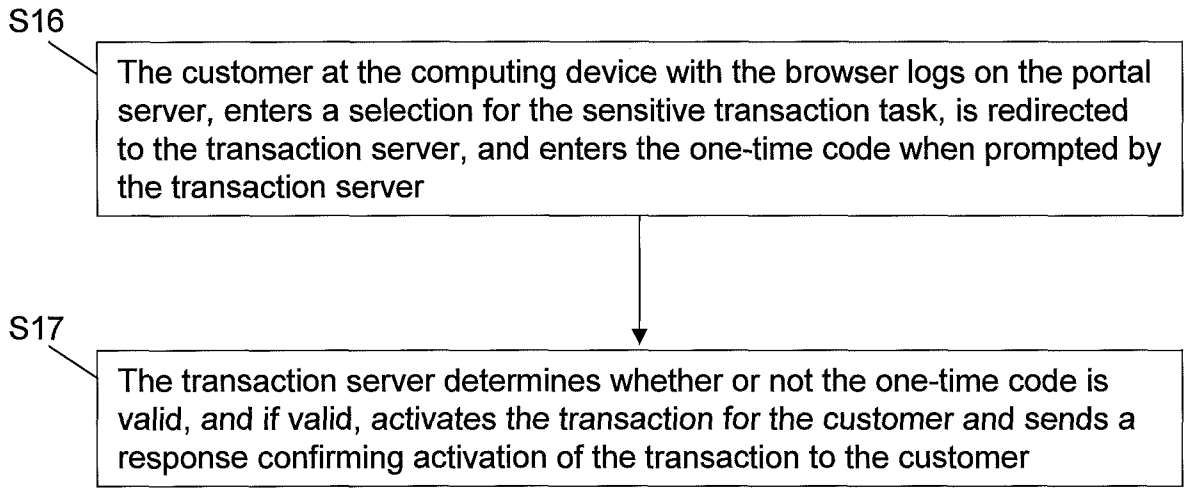
S16
The customer at the computing device with the browser logs on the portal server, enters a selection for the sensitive transaction task, is redirected to the transaction server, and enters the one-time code when prompted by the transaction server
S17
The transaction server determines whether or not the one-time code is valid, and if valid, activates the transaction for the customer and sends a response confirming activation of the transaction to the customer

FIG. 4

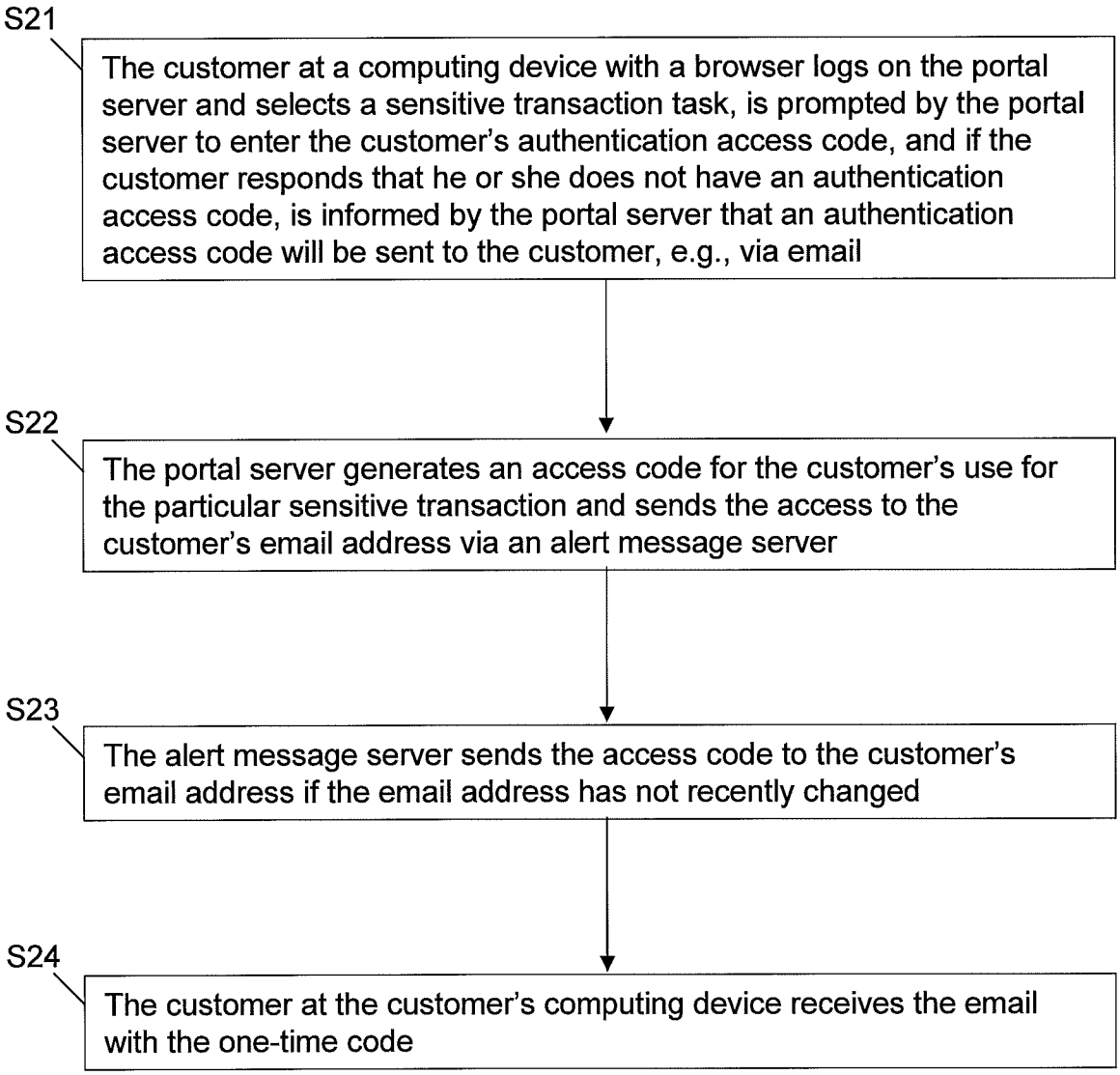
S21
The customer at a computing device with a browser logs on the portal server and selects a sensitive transaction task, is prompted by the portal server to enter the customer's authentication access code, and if the customer responds that he or she does not have an authentication access code, is informed by the portal server that an authentication access code will be sent to the customer, e.g., via email
S22
The portal server generates an access code for the customer's use for the particular sensitive transaction and sends the access to the customer's email address via an alert message server
S23
The alert message server sends the access code to the customer's email address if the email address has not recently changed
S24
The customer at the customer's computing device receives the email with the one-time code

FIG. 5

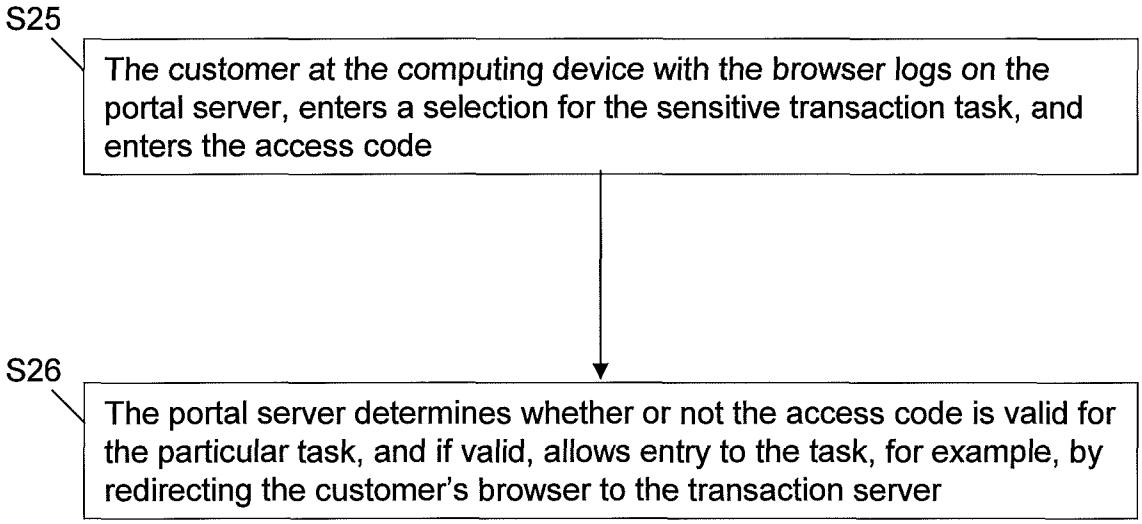
S25
The customer at the computing device with the browser logs on the portal server, enters a selection for the sensitive transaction task, and enters the access code
S26
The portal server determines whether or not the access code is valid for the particular task, and if valid, allows entry to the task, for example, by redirecting the customer's browser to the transaction server

FIG. 6

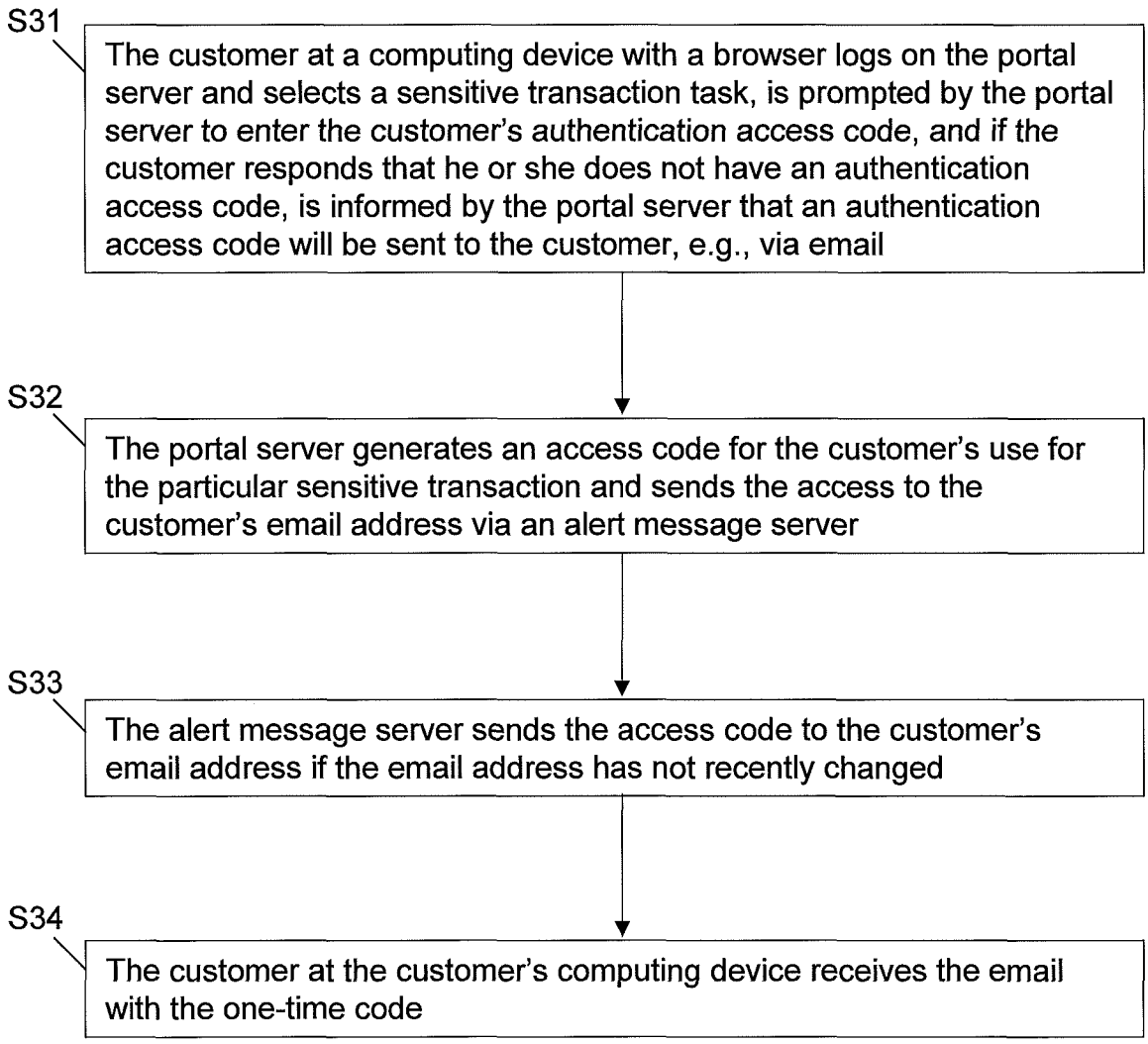
S31
The customer at a computing device with a browser logs on the portal server and selects a sensitive transaction task, is prompted by the portal server to enter the customer's authentication access code, and if the customer responds that he or she does not have an authentication access code, is informed by the portal server that an authentication access code will be sent to the customer, e.g., via email
S32
The portal server generates an access code for the customer's use for the particular sensitive transaction and sends the access to the customer's email address via an alert message server
S33
The alert message server sends the access code to the customer's email address if the email address has not recently changed
S34
The customer at the customer's computing device receives the email with the one-time code

FIG. 7

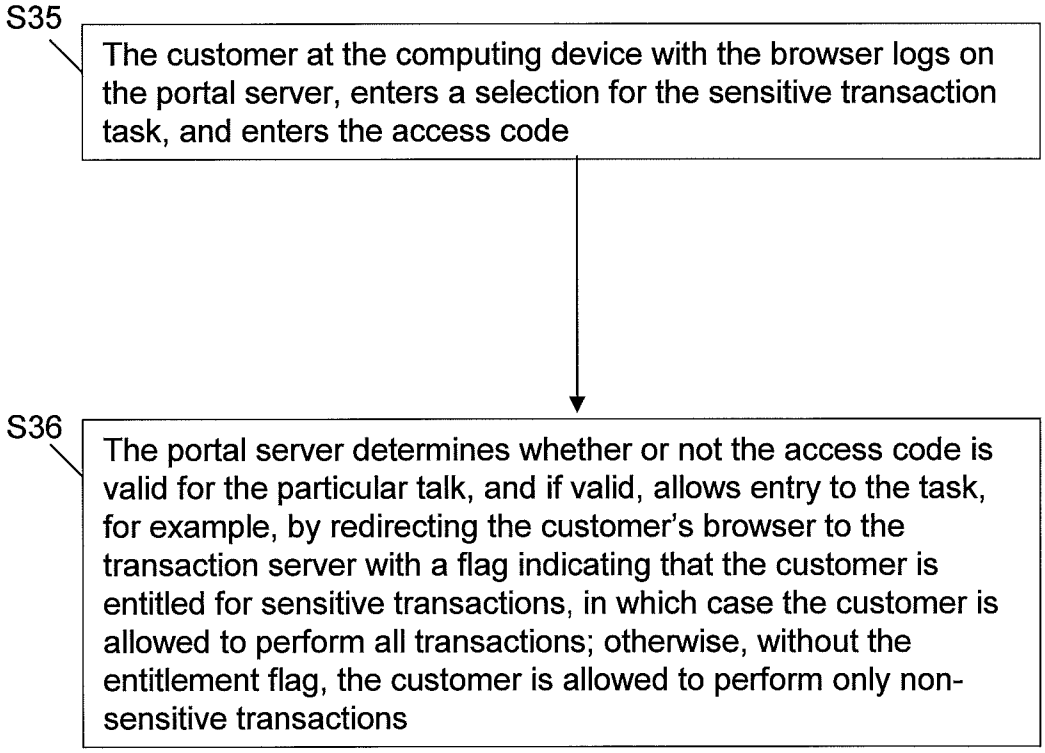
S35
The customer at the computing device with the browser logs on the portal server, enters a selection for the sensitive transaction task, and enters the access code
S36
The portal server determines whether or not the access code is valid for the particular talk, and if valid, allows entry to the task, for example, by redirecting the customer's browser to the transaction server with a flag indicating that the customer is entitled for sensitive transactions, in which case the customer is allowed to perform all transactions; otherwise, without the entitlement flag, the customer is allowed to perform only non-sensitive transactions

FIG. 8

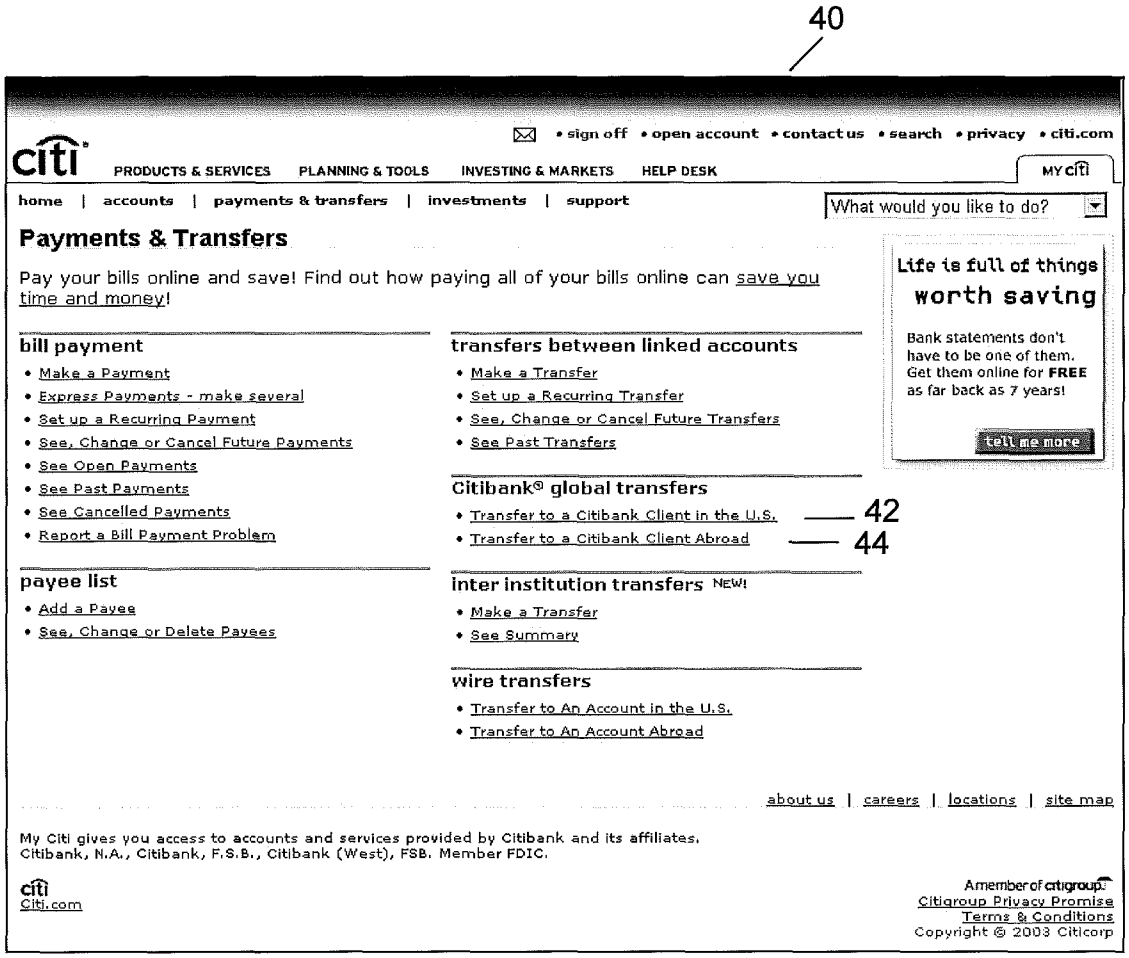
40
citi
• sign off • open account • contact us • search • privacy • citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Payments & Transfers
Pay your bills online and save! Find out how paying all of your bills online can save you time and money!
bill payment
• Make a Payment
• Express Payments - make several
• Set up a Recurring Payment
• See, Change or Cancel Future Payments
• See Open Payments
• See Past Payments
• See Cancelled Payments
• Report a Bill Payment Problem
payee list
• Add a Payee
• See, Change or Delete Payees
transfers between linked accounts
• Make a Transfer
• Set up a Recurring Transfer
• See, Change or Cancel Future Transfers
• See Past Transfers
Citibank® global transfers
• Transfer to a Citibank Client in the U.S.
• Transfer to a Citibank Client Abroad
42
44
inter institution transfers NEW!
• Make a Transfer
• See Summary
wire transfers
• Transfer to An Account in the U.S.
• Transfer to An Account Abroad
Life is full of things worth saving
Bank statements don't have to be one of them. Get them online for FREE as far back as 7 years!
tell me more
about us | careers | locations | site map
My Citi gives you access to accounts and services provided by Citibank and its affiliates. Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC.
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 9

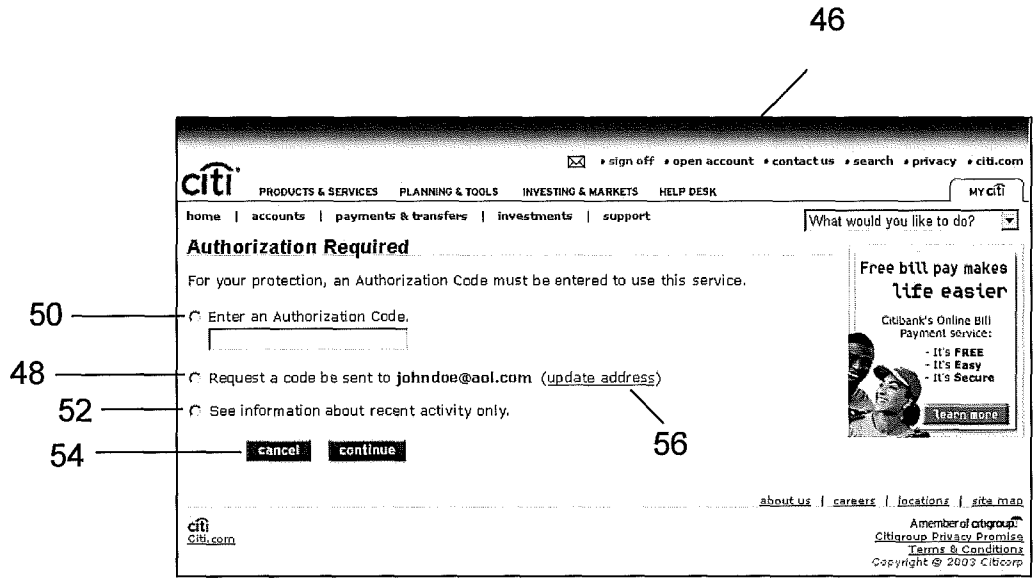
46
50
48
52
54
56
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Authorization Required
For your protection, an Authorization Code must be entered to use this service.
Enter an Authorization Code.
Request a code be sent to johndoe@aol.com (update address)
See information about recent activity only.
cancel
continue
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 10

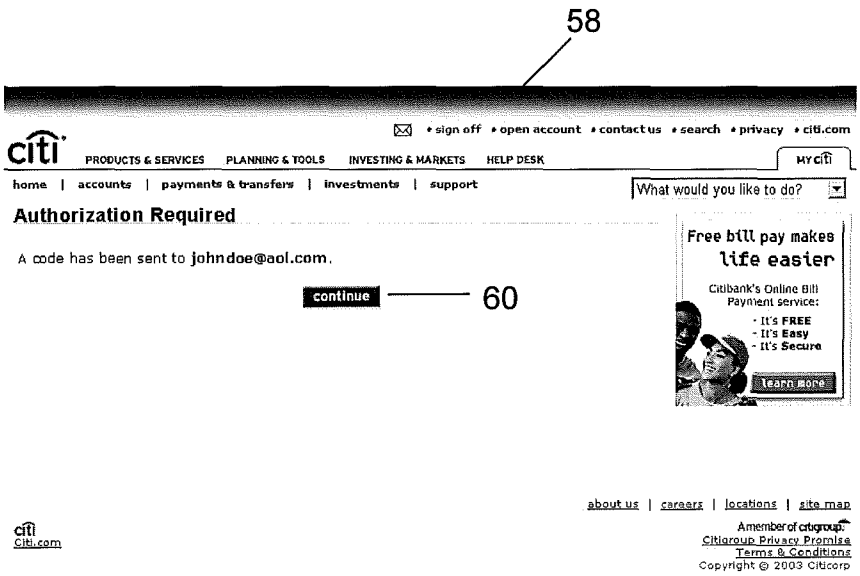
58
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Authorization Required
A code has been sent to johndoe@aol.com.
continue
60
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 11

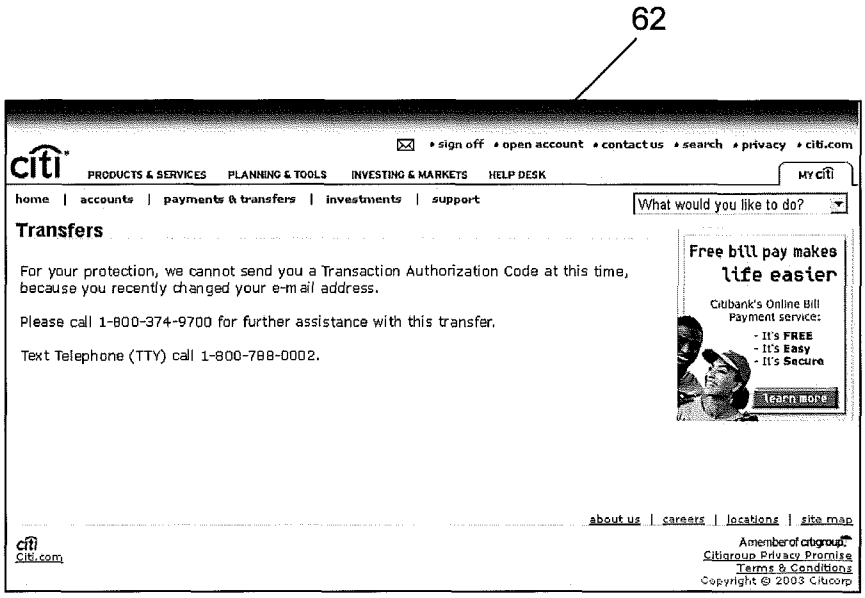
62
citi
sign off
open account
contact us
search
privacy
citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Transfers
For your protection, we cannot send you a Transaction Authorization Code at this time, because you recently changed your e-mail address.
Please call 1-800-374-9700 for further assistance with this transfer.
Text Telephone (TTY) call 1-800-788-0002.
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
Learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 12

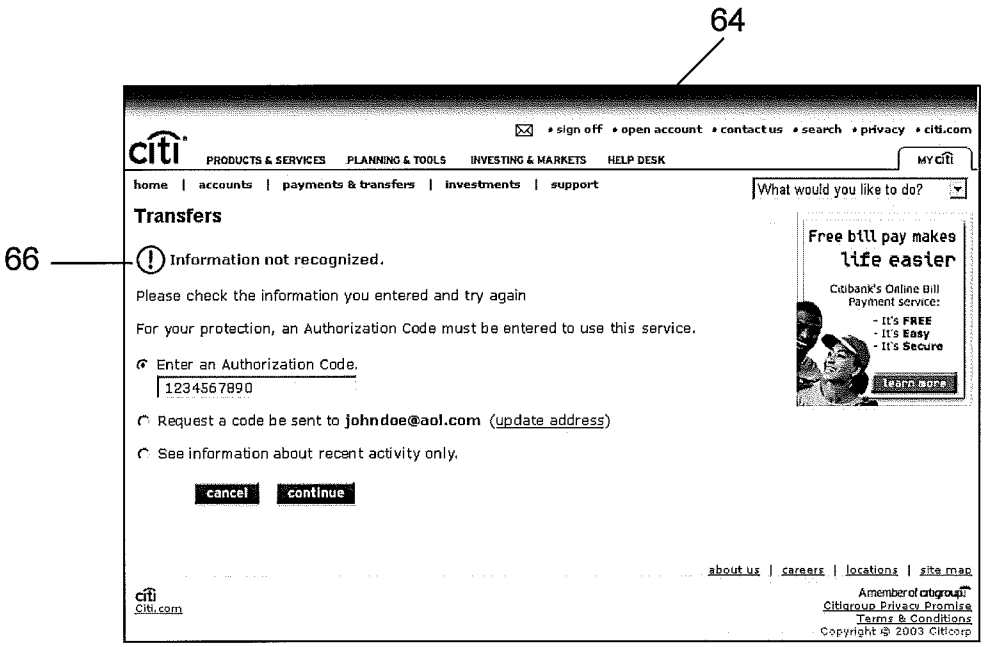
64
66
sign off
open account
contact us
search
privacy
citi.com
citi
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Transfers
Information not recognized.
Please check the information you entered and try again
For your protection, an Authorization Code must be entered to use this service.
Enter an Authorization Code.
1234567890
Request a code be sent to johndoe@aol.com (update address)
See information about recent activity only.
cancel
continue
Free bill pay makes life easier
Citibank's Online Bill Payment service:
- It's FREE
- It's Easy
- It's Secure
learn more
about us | careers | locations | site map
citi
Citi.com
A member of citigroup
Citigroup Privacy Promise
Terms & Conditions
Copyright © 2003 Citicorp

FIG. 13

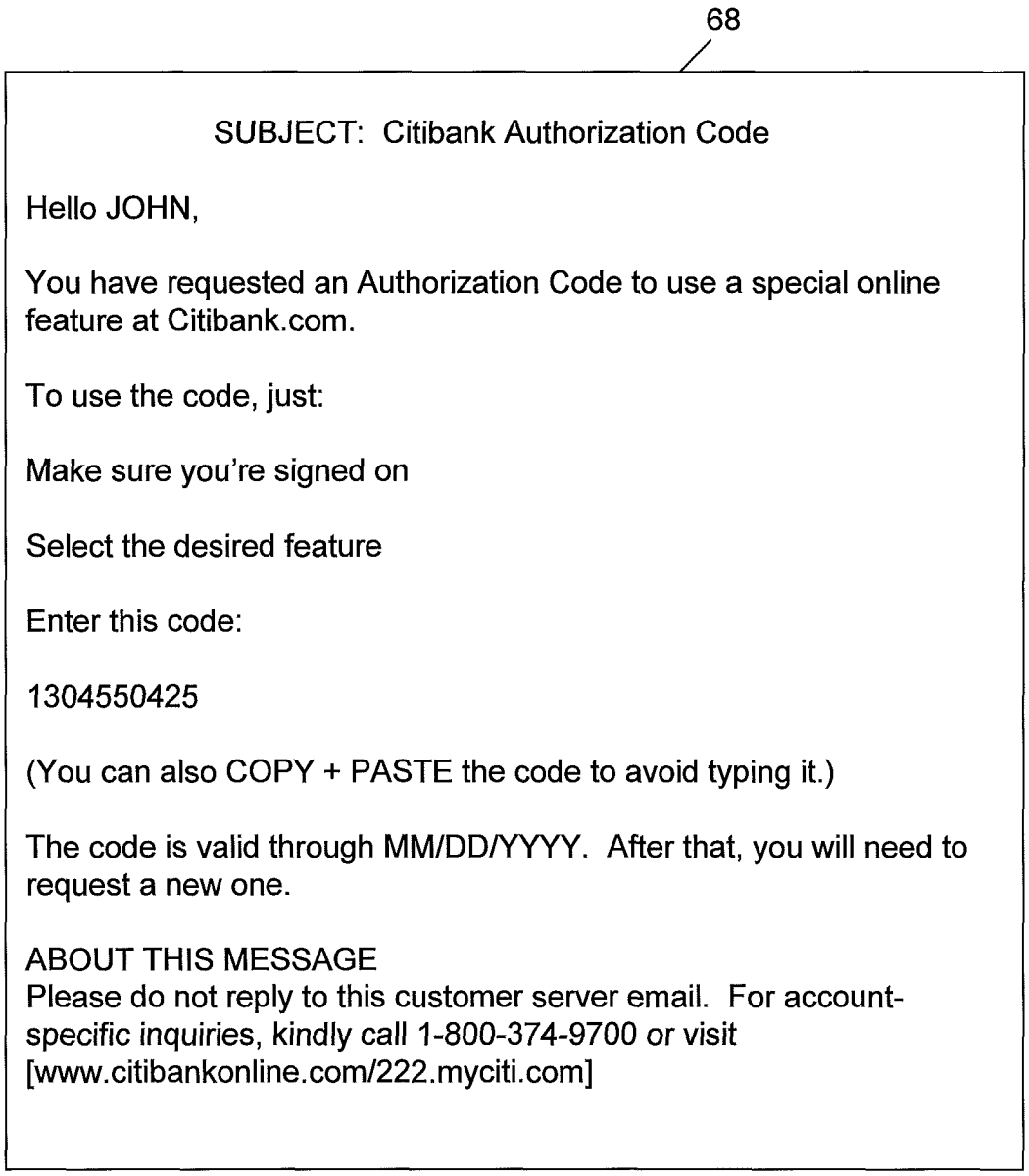
68
SUBJECT: Citibank Authorization Code
Hello JOHN,
You have requested an Authorization Code to use a special online feature at Citibank.com.
To use the code, just:
Make sure you're signed on
Select the desired feature
Enter this code:
1304550425
(You can also COPY + PASTE the code to avoid typing it.)
The code is valid through MM/DD/YYYY. After that, you will need to request a new one.
ABOUT THIS MESSAGE
Please do not reply to this customer server email. For account-specific inquiries, kindly call 1-800-374-9700 or visit [www.citibankonline.com/222.myciti.com]

FIG. 14

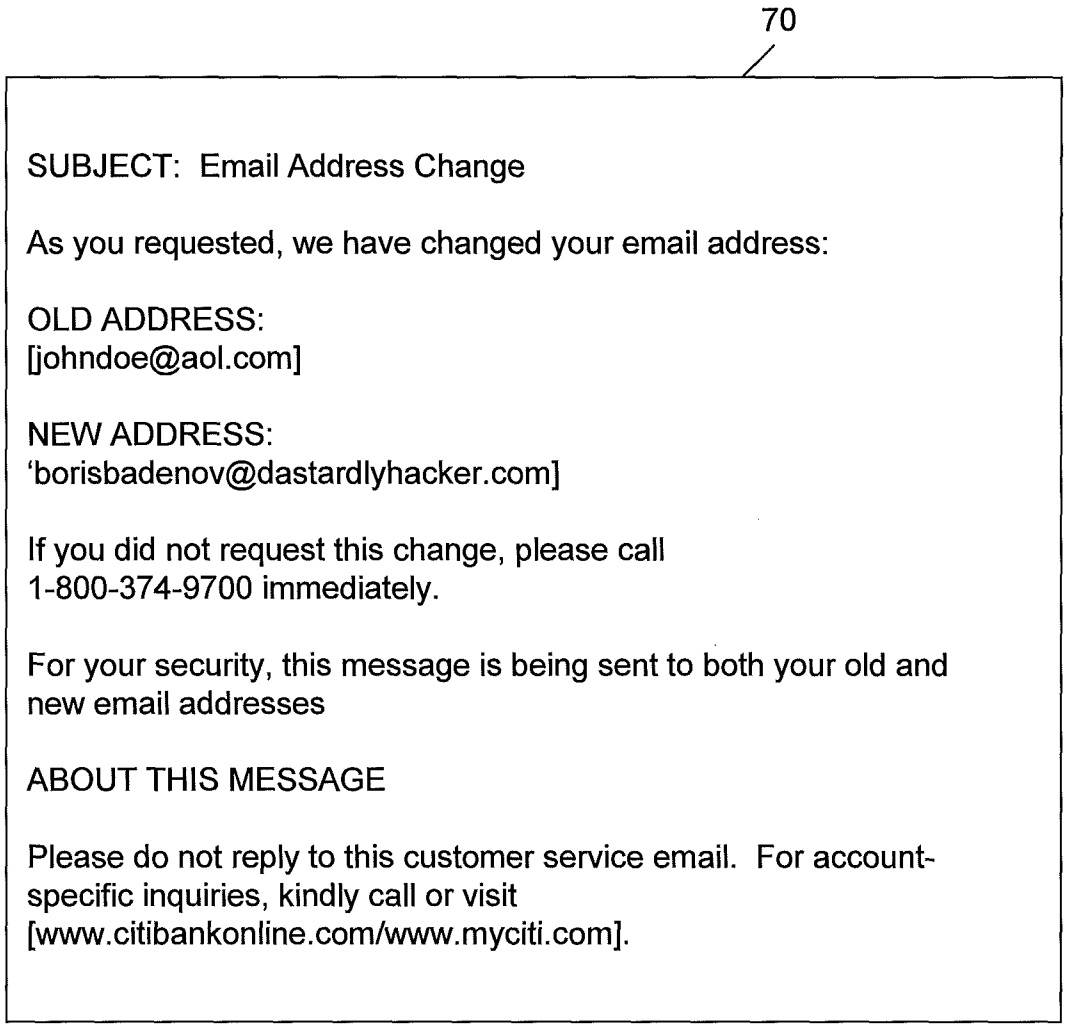
70
SUBJECT: Email Address Change
As you requested, we have changed your email address:
OLD ADDRESS:
[johndoe@aol.com]
NEW ADDRESS:
'borisbadenov@dastardlyhacker.com]
If you did not request this change, please call
1-800-374-9700 immediately.
For your security, this message is being sent to both your old and new email addresses
ABOUT THIS MESSAGE
Please do not reply to this customer service email. For account-specific inquiries, kindly call or visit
[www.citibankonline.com/www.myciti.com].

FIG. 15

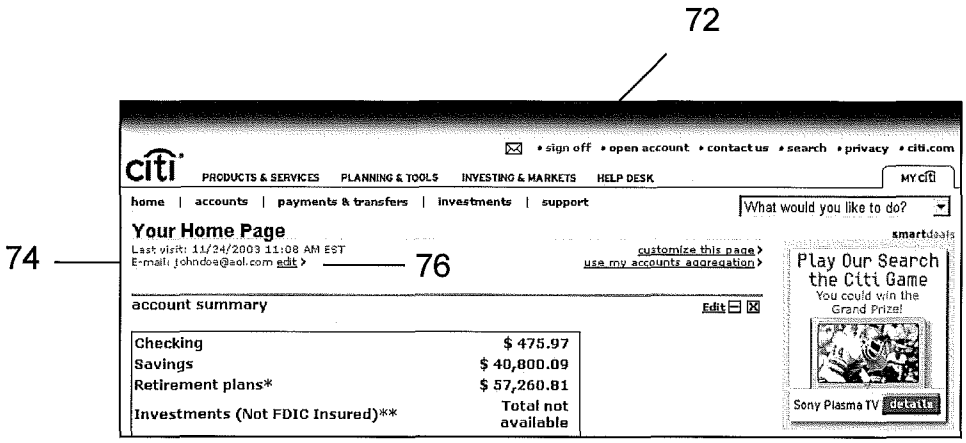
72
74
76
citi
• sign off • open account • contact us • search • privacy • citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MY citi
home | accounts | payments & transfers | investments | support
What would you like to do?
Your Home Page
Last visit: 11/24/2003 11:08 AM EST
E-mail: johndoe@aol.com edit >
customize this page >
use my accounts aggregation >
smartdeals
Play Our Search the Citi Game
You could win the Grand Prize!
Sony Plasma TV details
account summary
Edit
Checking $ 475.97
Savings $ 40,800.09
Retirement plans* $ 57,260.81
Investments (Not FDIC Insured)** Total not available

FIG. 16

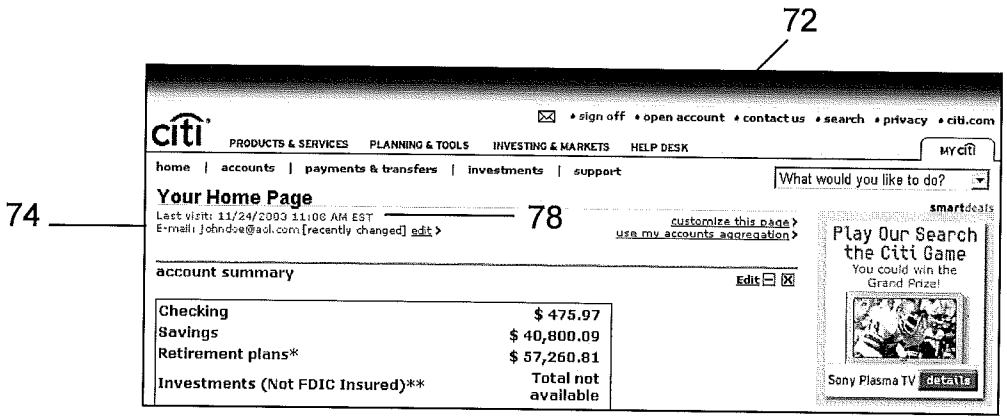
72
74
78
citi
sign off
open account
contact us
search
privacy
citi.com
PRODUCTS & SERVICES
PLANNING & TOOLS
INVESTING & MARKETS
HELP DESK
MYciti
home | accounts | payments & transfers | investments | support
What would you like to do?
Your Home Page
Last visit: 11/24/2003 11:06 AM EST
E-mail: johndoe@aol.com [recently changed] edit >
customize this page >
use my accounts aggregation >
smartdeals
Play Our Search the Citi Game
You could win the Grand Prize!
Sony Plasma TV details
account summary
Edit
Checking $ 475.97
Savings $ 40,800.09
Retirement plans* $ 57,260.81
Investments (Not FDIC Insured)** Total not available

FIG. 17

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 0111450 A **[0006]**

715949/KOT

ELJÁRÁSOK ÉS RENDSZEREK BIZTONSÁGOS FELHASZNÁLÓ HITELESÍTÉSRE

Szabadalmi igénypontok

1. Számítógép által megvalósított eljárás elektronikus kereskedelemben való biztonságos felhasználó hitelesítésre, amely a következőket tartalmazza:

elektronikus információ fenntartása, amelynek van egy első szempontja és egy második szempontja, az első szempont elérhető a felhasználó által egy első elektronikus kommunikációs csatornán a felhasználó által ismert első igazolvány bevitelére való válaszul, illetve a második szempont elérhető a felhasználó által az első elektronikus kommunikációs csatornán a felhasználónak biztosított második igazolvány bevitelére való válaszul;

kézbesítési cím előzetes bejegyzése egy második elektronikus kommunikációs csatornán, amely különböző az első elektronikus kommunikációs csatornától a felhasználó számára a második igazolvány biztosításához;

annak a lehetővé tétele egy felhasználó számára, hogy hozzáférjen az elektronikus információ első szempontjának aktuális folyamatához az első igazolvány bevitelére való válaszul és a második igazolvány biztosítása a felhasználó számára az előzetes bejegyzett kézbesítési címen a második elektronikus kommunikációs csatornán keresztül egy előre meghatározott felhasználó-választás bevitelére való válaszul az első szemponthoz való felhasználói hozzáférés folyamata alatt, ahol a felhasználó kézbesítési címében történő változás a második kommunikációs csatornán azt eredményezi, hogy egy jelző beállítódik egy tárolt profilon, megtiltva a második igazolvány biztosítását a felhasználó részére, ahol a jelző egy előre meghatározott időtartam utáni lejáratra állítódik be, és

egy folyamat engedélyezése a felhasználó számára, hogy hozzáférjen az elektronikus információ második szempontjához az első elektronikus kommunikációs csatornán keresztül a második igazolványnak a bevitelére való válaszul az egyik aktuális felhasználói, első szemponthoz való hozzáférési folyamat alatt, valamint

az első szemponthoz való felhasználói hozzáférés ezt követő folyamatának engedélyezése.

2. Az 1. igénypont szerinti eljárás, ahol az első szempont továbbá tartalmazza az elektronikus információ előre kiválasztott nem érzékeny tranzakciós szempontjait, a második szempont pedig továbbá tartalmazza az elektronikus információ előre kiválasztott érzékeny tranzakciós szempontjait.

3. Az 1. igénypont szerinti eljárás, ahol az első elektronikus kommunikációs csatorna továbbá tartalmaz egy számító eszközt, amely egy globális hálózaton keresztül csatlakozik egy webhely-kiszolgálóhoz.

4. A 3. igénypont szerinti eljárás, ahol az első elektronikus kommunikációs csatorna továbbá tartalmazza a számító eszközt, amely a globális hálózaton keresztül csatlakozik egy tranzakciós kiszolgálóhoz a webhely-kiszolgálón keresztül.

5. Az 1. igénypont szerinti eljárás, ahol az első elektronikus kommunikációs csatorna továbbá tartalmaz egy önkiszolgáló pénzügyi lebonyolító végberendezést, amely egy önkiszolgáló pénzügyi lebonyolító végberendezés-hálózaton keresztül csatlakozik egy gazdagép-kiszolgálóhoz.

6. Az 1. igénypont szerinti eljárás, ahol az első igazolvány továbbá tartalmaz egy jelszót, amelyet a felhasználó választ ki a felhasználó azonosítására.

7. Az 1. igénypont szerinti eljárás, ahol a második igazolvány továbbá tartalmaz egy véletlenül előállított olyan titkos kódot a felhasználó azonosítására, amely biztosítva van a felhasználó számára.

8. Az 1. igénypont szerinti eljárás, ahol a második igazolvány biztosítva van a felhasználónak az elektronikus információ második szempontjához való önálló hozzáférés folyamata számára.

9. Az 1. igénypont szerinti eljárás, ahol a második igazolványnak van egy előre meghatározott lejárata, amely után a második azonosító igazolvány már nem érvényes az elektronikus információ második szempontjának eléréséhez.

10. Az 1. igénypont szerinti eljárás, ahol a kézbesítési cím előzetes bejegyzése a második elektronikus kommunikációs csatornán továbbá tartalmazza egy mobil távközlési eszköz előzetes bejegyzését és egy e-mail címet a második igazolványnak a felhasználó számára való biztosítására.

11. Az 1. igénypont szerinti eljárás, ahol a második igazolvány biztosítása a felhasználónak a második elektronikus kommunikációs csatornán keresztül továbbá tartalmazza a második igazolványnak a felhasználó részére szöveges üzenettel való biztosítását.

12. Az 1. igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára való biztosítása továbbá tartalmazza a második azonosító igazolványnak a felhasználó részére egy felhasználói kijelentkezésre való válaszul az első szemponthoz való felhasználói hozzáférés aktuális folyamatában történő lezárásakor.

13. A 12.igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára a felhasználói kijelentkezésre való válaszul történő biztosítása továbbá tartalmazza a második igazolványnak a felhasználó számára való biztosítását az első szemponthoz való felhasználói hozzáférés következő folyamata alatti használatra.

14. Az 1. igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára a felhasználó-választásra való válaszul történő biztosítása továbbá tartalmazza a második igazolványnak a felhasználó részére egy felhasználói kérésre való válaszul a második igazolványhoz az első szemponthoz való felhasználói hozzáférés aktuális folyamata alatti biztosítását.

15. Az 1. igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára a felhasználó-választásra való válaszul történő biztosítása továbbá tartalmazza a második igazolványnak a felhasználó részére az elektronikus információ második szempontjához

való felhasználói hozzáférési kísérletre való válaszul az első szemponthoz való felhasználói hozzáférés aktuális folyamata alatti biztosítását.

16. A 15. igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára a felhasználónak az elektronikus információ második szempontjának elérési kísérletére való válaszul történő biztosítása továbbá tartalmazza a második igazolványnak a felhasználó részére az elektronikus információ előre kiválasztott érzékeny tranzakciós szempontjaihoz való hozzáférési kísérletre való válaszul történő biztosítását.

17. A 16. igénypont szerinti eljárás, ahol a második igazolványnak a felhasználó számára az elektronikus információ előre kiválasztott érzékeny tranzakciós szempontjai elérési kísérletére való válaszul történő biztosítása továbbá tartalmazza a második igazolványnak a felhasználó számára az elektronikus információ előre kiválasztott érzékeny tranzakciós szempontjaihoz való felhasználói navigálási kísérletet.

18. Számítógépes rendszer elektronikus kereskedelemben való biztonságos felhasználó hitelesítésre, amely a következőket tartalmazza:

adattároló eszköz, amely elektronikus információt tárol, amelynek van egy első szempontja és egy második szempontja;

első elektronikus kommunikációs csatorna eszköz, amelyen keresztül az első szempont elérhető egy felhasználó által a felhasználó által ismert első igazolvány bevitelére való válaszul, és amelyen keresztül a második szempont elérhető a felhasználó által a felhasználónak biztosított második igazolvány bevitelére való válaszul;

második elektronikus kommunikációs csatorna eszköz, amely különböző az első elektronikus kommunikációs csatorna eszköztől a felhasználó számára a második igazolványnak egy előre bejegyzett kézbesítési címen való biztosításához;

az első elektronikus kommunikációs csatorna eszköz, amely arra van kialakítva, hogy lehetővé tegye a felhasználónak az elektronikus információ első szempontjának eléréséhez való aktuális folyamatot az első igazolvány bevitelére való válaszul, valamint a második igazolványnak a felhasználó számára az előre bejegyzett kézbesítési címen a második elektronikus kommunikációs csatornán keresztül egy

előre meghatározott felhasználói kiválasztásnak az első szemponthoz való felhasználói hozzáférés folyamata alatti bevitelére való válaszul történő biztosítására, ahol egy változás a felhasználói kézbesítési címben azt eredményezi, hogy beállítódik egy jelző egy tárolt profilon, amely megtiltja a második igazolványnak a felhasználó számára való biztosítását,

ahol a jelző egy előre meghatározott időtartam utáni lejáratra van beállítva, az első elektronikus kommunikációs csatorna eszköz pedig továbbá arra van kialakítva, hogy lehetővé tegye a felhasználó számára az elektronikus információ második szempontjához az első elektronikus kommunikációs csatornán keresztül a második igazolvány bevitelére való válaszul az első szemponthoz történő hozzáférés folyamatát az első szemponthoz való egyik aktuális felhasználói hozzáférési folyamat alatt, valamint az első szemponthoz való felhasználói hozzáférés következő folyamatát.