

user to be present before secure transactions can be conducted using the Extranet. A physical device used in this embodiment is shown in FIG. 8, which depicts a credit card sized compact disc 260 that, when present in the user's CD or DVD disk drive, can be used to authenticate the user to the EXN Server. A user's PAC can be encrypted upon the recorded digital medium of the disk 270. If desired, further validation of the user's identity may be recorded on the disk in the form of a confidential question and response protocol. As a convenience to the user, a modified disk may be fabricated to the dimensions of a standard credit card and a magnetic strip (or an optical equivalent) 280 can be affixed to the disc, thereby enabling it to be read by standard card reading equipment. In this embodiment, a "card present" signal must be received by the EXN Server before any transactions will be permitted.

[0088] In practice, the question and response protocol can be maintained on the CD as an encrypted file to be accessed with a PIN or other key, or the challenge and response information may be maintained on the EXN Server. Information exchanged in the challenge and response protocol, such as, for example, the name of a favorite pet, or a mother's maiden name, which would not be known to a hacker, is normally sufficient to verify the user, and such information could therefore be maintained on the EXN Server without fear of revealing the identification of the user. In this case, when the CD is placed into a disc drive, the user would be required to enter a PIN in order to activate the CD. Upon activation, the CD would establish a connection with the Extranet and identify the user with the user's PAC. The EXN Server would then commence a series of questions and answers that would have to be successfully completed before transactions would be accepted by the EXN Server. As the physical disc (or other physical medium) and virtual credentials are available and known only to the user, the likelihood that a hacker or unauthorized third party could obtain the physical and virtual credentials necessary to commit a fraudulent transaction through the Extranet is substantially eliminated. For example, a fraudulent transaction could not be made where the unauthorized user knows only a user's PAC. The fraudulent user could not gain access to the Extranet unless the physical card, the personal identification number to unlock the CD (PIN), and the correct answers to the challenge and response questions are all present and are known to the fraudulent user.

[0089] A similar physical security regimen can be implemented for mobile phone users through a portable card reader that can be connected to a mobile phone. Once a connection to the EXN Server is established, the challenge and response procedure can be carried out over the telephone, and the user can be authenticated to the EXN Server for financial transactions.

[0090] The registration of users of the Extranet is depicted in FIGS. 9 and 10. Registration is accomplished with the use of a temporary registration compact disc (CD) 290 that is distributed by the member bank 12 to the user. The method of registration takes place on two discrete levels: bank registration of the user with the user's bank, and Extranet registration of the user with the EXN Server.

[0091] In FIG. 9, the user must first open an account with a bank 12 having a contract with the EXN Operator 100. In one embodiment of this registration, the user provides the bank with personal information necessary to open the account and to subsequently identify the user as the owner

of that account. The user is then given an pre-registration compact disc (CD) 290 that contains an encoded pre-registration number that will be used temporarily to identify the user to the bank. Although a CD is a preferred embodiment of the invention, it is possible that some other physical medium may be used, such as a magnetic encoded plastic card or a microchip suitable for use with a cellular phone, a hybrid personal data assistant (PDA), or some other suitable communications device.

[0092] At the bank, the user's pre-registration number is cross-referenced to the user's bank account number so that the user may be identified in subsequent electronic transmissions. The CD typically will also include the bank's routing number or IP address (to provide the EXN Server with sufficient information to connect to the bank when the user registers with the EXN Server) and the user's encoded pre-registration number, but will not include the user's bank account number. In one embodiment of the invention, shown in FIG. 10, the user will insert the CD into a computer that will establish an internet connection with the bank. If the user successfully answers a series of challenge and response questions based upon information the user gave to the bank when opening the account, the bank will activate the CD (or will give the user information to activate the CD). Once the registration CD has been activated, the user will be able to contact the EXN Server and register to use the Extranet.

[0093] After activating the CD, the user will register with the EXN Server. Upon accessing the EXN Server 100, the user will provide information for the EXN Server to register the user and to notify the bank 12 that the user has been registered. This step may be accomplished in any number of ways, including having the EXN Server communicate with the user's bank using the pre-registration number previously assigned to the user's CD; alternatively, the user may be identified to the bank with a bank-issued PAC or through personal information provided by the user. If it has not already occurred, during this phase of the registration, a PAC will be generated, and will thereafter permanently identify the user to the EXN Server and, in some embodiments, to the user's bank. If a single user has multiple accounts, a unique PAC may optionally be issued to identify each of the user's accounts.

[0094] The operation of the Extranet of this invention may be demonstrated in the following typical consumer purchase transaction that is conducted on-line across the internet. During the "boot up" process, the computer will automatically establish a connection with the EXN Server, notifying the server that the user's computer is on line. Alternatively, a user can manually establish a connection to the EXN Server, as when the user is using a guest computer. Once a connection with the EXN Server has been established, the user will be authenticated, and the EXN Server will be able to communicate with the user's computer during a shopping session.

[0095] The on-line transaction may commence with a Purchaser's conversion of available funds in the Purchaser's bank account into e-cache that can be used on-line in connection with the Extranet of this invention. The use of a vATM and its corresponding real world transaction are previously described in FIGS. 2a and 2b, and will result in a purchaser's having e-cache in an eWallet to make an on-line purchase.

[0096] The transaction continues as shown in FIG. 11 in which the purchaser 30 is making an on-line purchase. The