

25

returning the encrypted data combination to the client computer.

54. A computer-readable storage medium as recited in claim 53, data item is derived from a user logon secret supplied during the network logon procedure.

55. A computer-readable storage medium as recited in claim 53, containing instructions for performing an additional step of creating a message authentication code based at least in part on the data item and the user identification, the data combination further including the message authentication code.

56. A computer-readable storage medium as recited in claim 53, wherein the encrypting step is performed using an encryption key that is derived from a master key and a random key, the instructions being executable to perform an additional step of returning the random key with the encrypted data combination to the client computer.

57. A computer-readable storage medium as recited in claim 53 containing further instructions for performing additional steps comprising:

creating a message authentication code based at least in part on the data item and the user identification, the data combination further including the message authentication code, wherein the message authentication code is created using an authentication key that is derived from a master key and a random key;

returning the random key with the encrypted data combination to the client computer.

58. A computer-readable storage medium as recited in claim 53 containing further instructions for performing additional steps comprising:

creating a message authentication code based at least in part on the data item and the user identification, the data combination further including the message authentication code, wherein the message authentication code is

26

created using an authentication key that is derived from a master key and a first random key;

wherein the encrypting step is performed using an encryption key that is derived from a master key and a second random key;

returning the first and second random keys with the encrypted data combination to the client computer.

59. A computer-readable storage medium containing instructions that are executable by a network client to perform steps comprising:

deriving a client key from a user secret that is supplied by a user during network logon procedures;

securing user data with the client key;

sending the client key to a network supervisory computer that authenticates network users during user logon procedures;

in response to sending the client key, receiving an encrypted data combination from the network supervisory computer, the encrypted data combination being decryptable by the network supervisory computer to obtain the client key, wherein the encrypted data combination is not decryptable by the network computer; storing the encrypted data combination for use in recovering the client key when the user secret changes.

60. A computer-readable storage medium as recited in claim 59 containing further instructions for performing an additional step of sending the encrypted data combination to the network supervisory computer in order to recover the client key.

61. A computer-readable storage medium as recited in claim 59 containing further instructions for performing an additional step of encrypting the client key before sending it to the network supervisory computer.

* * * * *