

return the hardcopy certificate to the customer or print "VOID" on the hardcopy certificate and store it locally.

[0130] The ASD 105 has a network interface device 181 for communicating with the remote ASD host 101 (e.g., modem, wireless interface, Ethernet interface). The ASD 105 has additional devices for management and administration purposes: a console (with display and keyboard) or a input-output port at which to connect a console; and a back-up battery 171 to allow continued operation and proper closing down in the event of main power failure. The print/scan device 163 also prints out paper records of transactions for auditing purposes.

[0131] Communications between the ASD 105 and the securities dealing financial institution is made secure through the use of encryption techniques. Let K_A denote the cryptographic key used for securing the communications between the ASD 105 and the security dealing financial institution. (K_A would be a random number whose length depends on the encryption algorithm, e.g., 56 bits in DES, 128 bits or higher in AES.) K_A is stored in the ASD's cryptoprocessor non-volatile memory and in the securities dealing financial institution's computer, and perhaps authorized key escrow agents).

[0132] When the securities dealing financial institution sends data, say X , to the ASD, it first encrypts the data with K_A and transmits the encrypted data, i.e., transmits $E(K_A, X)$, where E is the encryption algorithm (e.g., DES, AES). When the ASD 105 receives $E(K_A, X)$, it forwards the message to its cryptoprocessor, which decrypts $E(K_A, X)$ using K_A to extract X (i.e., computes $D(K_A, E(K_A, X))$, where D is the decryption function) and passes X to the ASD 105 computer. Note that the ASD 105 computer never gets to see K_A , so a compromise of the ASD 105 computer does not compromise K_A .

[0133] The same procedure is followed when the ASD 105 sends data to the securities dealing financial institution. The ASD computer 131 uses the cryptoprocessor 141 to encrypt the data with key K_A , and transmits the encrypted data to the securities dealing financial institution.

[0134] When $E(K_A, X)$ is transmitted (either by the ASD 105 or the securities dealing financial institution), an eavesdropper on the communication link can obtain $E(K_A, X)$, but not X because the eavesdropper does not know K_A (obtaining X from $E(K_A, X)$ without knowing K_A is computationally infeasible). Furthermore, if the message $E(K_A, X)$ is intercepted and modified, then when the modified message is received and decrypted, the resulting data will be garbled (i.e., will not have the appropriate structure of X), and so the receiver will discard it. Further protection against message modification can be achieved by including in the message a cryptographic checksum generated from the contents of the message and a cryptographic key (this key is distinct from K_A or the key used in protecting certificates).

[0135] The software executed by the main computer 131 of the ASD 105 includes an operating system and applications software. The operating system (e.g., Windows 2000, Linux) implements a platform on which applications software execute and control the input-output devices (e.g., issue commands to the printer-scanner, do TCP/IP networking).

[0136] The applications software includes procedures for handling "buy" and "sell" operations by the customer. These

procedures prompt the customer for inputs and issue outputs, interact with the remote ASD host 101 over the network connection, and ensure that the ASD 105 and the ASD host 101 have a consistent view of the sequence of transactions performed, i.e., at the end of a transaction, either both sides have successfully completed it or both sides have completely cancelled the operation.

[0137] The applications software also includes secure networking software (e.g., Secure Shell, SSH) that ensures that the ASD's interaction with the remote ASD host 101 is authenticated, encrypted, and protected from intentional or accidental modification. The encryption itself is done by the cryptoprocessor 141. The applications software further can include optical character recognition (OCR) for verifying the cryptographic checksum therein (rather than at the ASD host 101 or the securities dealing financial institution).

[0138] To ensure that a printed hardcopy certificate is unmodifiable, the system uses cryptographic techniques. Specifically, it prints a cryptographic checksum (i.e., cryptographically-strong integrity checksum) on the hardcopy certificate, for example "30984763982847223945732834587" in FIG. 14. In practice, the checksum would be larger. The checksum is printed on the hardcopy certificate as a sequence of numbers or as a barcode. Producing an unmodifiable hardcopy certificate does not require special paper or high-resolution printing. The checksum is computed by applying a cryptographic algorithm (e.g., keyed-hash message authentication code (HMAC) with Secure Hash Algorithm (SHA)) to the information on the hardcopy certificate and a cryptographic key (a large number) that is held in secret by the securities dealing financial institution. This key is referred to as the certificate key (which is different from the cryptographic key that the ASD 105 uses for secure communications with the ASD 105 host). The book entitled "Network Security: Private Communication in a Public World", 2nd edition, by Kaufman, Perlman, and Speciner, ISBN 0-13-046019-2, provides guidance in developing a suitable algorithm (e.g., HMAC).

[0139] Unmodifiability of the information of a printed hardcopy certificate is achieved by the use of an appropriate cryptographic algorithm, for example, a keyed-hash function. Let K_B denote the certificate key, i.e., the large random number that is held in secret by the securities dealing financial institution and used in computing the checksum for a hardcopy certificate. Let Y be the information, excluding the checksum, to be printed on a hardcopy certificate. Then the checksum for the hardcopy certificate is a large number, say $H(K_B, Y)$, obtained by applying a keyed-hash function H (e.g., HMAC with SHA) to the key K_B and the data Y .

[0140] When the certificate is printed, the securities dealing financial institution sends Y as well as $H(K_B, Y)$, and the ASD 105 prints Y and $H(K_B, Y)$ on the hardcopy certificate. H is such that it is computationally infeasible to obtain $H(K_B, Y)$ without knowing K_B or to modify Y to say Z such that $H(K_B, Z)$ equals $H(K_B, Y)$. Thus the information on the hardcopy certificate cannot be changed without the checksum becoming invalid. Because Y and $H(K_B, Y)$ are sent to the ASD 105 in an encrypted protected message, an attacker cannot modify the message while in transit (as explained above). Thus the printed hardcopy certificate is unmodifiable.