

[0141] The certificate key  $K_B$  is usually different from the key  $K_A$  used to secure communications between the ASD 105 and the ASD 105 host. The securities dealing financial institution can also use different  $K_B$ 's for different classes of certificates (to limit the damage in case a certificate key is compromised).

[0142] The keyed-hash function is such that (1) any changes to the information on the document (such as modifying the face value) makes the checksum invalid, and (2) the valid checksum for the modified document cannot be obtained without knowing the key. Thus the checksum ensures that any modification to the information of the hardcopy certificate can be easily detected. A cryptographic checksum can also be computed using encryption functions, e.g., Data Encryption Standard (DES), Advanced Encryption Standard (AES), etc.; typically the data to be protected is encrypted with the certificate key and the final cipherblock (also called residue) is used as the checksum.

[0143] The checksum computation can be done at the securities dealing financial institution and the result then sent to the ASD 105 for printing on the hardcopy certificate. Alternatively, the computation can be done in the ASD's cryptoprocessor (in which case the cryptoprocessor would have a copy of the certificate key).

[0144] When achieving unforgeability of a printed hardcopy certificate involves taking a scan of the printed hardcopy certificate, the analysis is the same as that for unmodifiability, except that the fingerprint characterizes the printed image of the hardcopy certificate (including the random pattern embedded in the paper) rather than only the information on the hardcopy certificate.

[0145] To ensure that a printed hardcopy certificate is unforgeable, the system uses special paper. The use of special paper requires stocking the special paper. There are many types of special papers, including paper with security fibers (colored, metallic or fluorescent), paper with embedded holograms, and paper with microprinting. One can resort to paper of increasing specialization for certificates of increasing face value.

[0146] To increase the difficulty of forging a document, a random pattern is printed/embedded in the paper and the pattern will be recorded when the certificate is issued. For example, the special paper randomly embedded with colored fibers as shown in FIG. 15. To print an unforgeable hardcopy certificate, the ASD 105 uses a sheet of this special paper, records a digital scan of the hardcopy certificate, and forwards this scan to the securities dealing financial institution for storage. A duplicate of the printed security would be detectable because, even if the forger had access to the same kind of special paper, it is highly unlikely that the sheet of special paper used for the forgery would have the same random embedding of colored fibers.

[0147] An example of a "buy" operation according to the invention is explained as follows. A customer walks up to an ASD, inputs information that specifies the certificate to buy (e.g., bond X of value Y), the method of payment (e.g., debit card and PIN number), and the customer's identity (e.g., name and address). The ASD 105 contacts the securities dealing financial institution, provides payment information, and receives the details of the certificate to be printed (including the cryptographic checksum, whether it is to be

printed on special paper, and if so, whether a scan is to be taken). It then prints the hardcopy certificate, dispenses the hardcopy certificate to the customer, and informs the dealing financial institution of the completion of transaction. The ASD 105 obtains a scan of the printed hardcopy certificate so printed before dispensing it to the customer, and transmits the scan to the securities dealing financial institution (via ASD 105 host) for long-term storage before finishing the transaction.

[0148] FIG. 16 provides the details of the "Buy" procedure as executed by the computer 131. Operations that involve either input or output with the customer or with the ASD host 101 are tagged as such. As usual, an input operation usually involves also some output. For example, in a Step 1, the ASD 105 displays a welcome message to start a buy transaction with a customer. In a Step 2, the user inputs his/her background information, such as name, address, social security number, etc. In a Step 3, the user inputs details of desired certificate, such as issuing company, face value, duration of certificate, etc. In a Step 4, a keycard input is preceded by a prompt on the display to the customer requesting to input the card to get details of payment method, such as bank account number, PIN, etc. if to pay by a debt card. The ASD 105 starts a transaction with the ASD host 101 by sending a network output to the ASD host 101 involving a handshake between the ASD 105 and the ASD 105 host (Step 5), and then sends details of desired certificate to the ASD host 101 (Step 6). Thereafter, the ASD 105 receives a reply from the ASD host 101 via the network (Step 7). If the ASD host's reply indicates the certificate is not available in the database, the ASD 105 informs customer by displaying the results (Step 8). If ASD host's reply indicates the certificate is available in the database, the ASD 105 sends the payment information to the ASD host 101, receives reply from the ASD host 101 indicating what to print (including a cryptographic checksum), type of paper to use, and whether a scan is to be taken. Thereafter, the ASD 105 prints a certificate on a proper paper via the print-scan device 163, as well as scans the certificate if required by the ASD host 101 and sends scanned image to the ASD host 101 accordingly. The ASD 105 dispenses a printed hardcopy certificate to the customer (Step 9). The ASD 105 prints transaction status on a local printer for recording keeping (Step 10), ends the transaction with the ASD host 101 (Step 11), and ends the transaction with the customer by displaying a message of "transaction completed".

[0149] Step 1: "start transaction with ASD 105 host" and Step 12: "end transaction with ASD 105 host" demarcate the transaction that is to be "atomically" executed with the ASD 105 host; i.e., if the transaction is not completed successfully (say the communication link failed), the state at the start of transaction is restored at both the ASD 105 and the ASD 105 host.

[0150] An example of a "sell" operation according to the invention is explained as follows. A customer walks up to an ASD, inserts the printed hardcopy certificate to be sold into the print/scan device 163 of the ASD, and inputs payment information (i.e., account to which payment is to be deposited). The ASD 105 scans the document and forwards the scan and the payment information to the securities dealing financial institution. The dealing financial institution verifies the cryptographic checksum and the scan (if applicable). If the verification is successful, the dealing financial institution