A SYSTEM AND METHOD FOR AUTHENTICATING IDENTITIES OVER REMOTE CHANNELS

162162

ABSTRACT

[0043] A system for authenticating identity of a user, comprising: an authentication server having a true random number generator and a storing means, the authentication server for generating a sequence of true random numbers; the sequence of true random numbers for deriving a sequence of server passwords by subjecting the sequence of true random numbers to a predetermined one-way function, for authenticating identity of the user; a token for storing the sequence of true random numbers for accessing by the user; a token reader coupled to a displaying means for accessing the token; wherein, the token reader upon activation with the token accesses the token for a first of the sequence of true random numbers and deleting the first of the sequence of true random numbers from the token before displaying the first of the sequence of true random numbers on the displaying means; further wherein, the authentication server upon positive authentication of the user by comparing the first of the sequence of true random numbers from the token and any of the sequence of server passwords from the storing means for a matching server password and deleting the matching server password and all preceding server passwords from the sequence of server passwords from the storing means of the authentication server.

[0044] FIG.1 accompanies the abstract.