ABSTRACT

ONE TIME PASSWORD

A token calculates a one time password by generating a HMAC-SHA-1 value based upon a key K and a counter value C, truncating the generated HMAC-SHA-1 value modulo 10^Digit, where Digit is the number of digits in the one time password. The one time password can be validated by a validation server that calculates its own version of the password using K and its own counter value C'. If there is an initial mismatch, the validation server compensate for a lack of synchronization between counters C and C' within a look-ahead window, whose size can be set by a parameter s.