Abstract

We present a method of generation of one-time keys (OTK) for single line authentication using zero knowledge (ZK) computation as undertaken by an authentication client application on a mobile device and a registration server. The method comprises initiation of an activation process on the authentication client by a user associated with the mobile device, a ZK computation sequence on the authentication client for generation of storage key and transport key, transportation of the ZK computation outcome to the browser, user input into a text-entry element, and then additional server-side processing for association of the authentication client on the mobile device. This would be inclusive of ZK computations for the user identifier (UID), a user-associated hashed message authentication code (HMAC) key for subsequent authentication interactions, and additionally a transport key, for secure server-to-device transmission these user-specific parameters on an out-of-band (OOB) channel as presumed to be insecure. Thereafter, additional ZK computations are undertaken client-side for recovery of UID and the HMAC key, and following that insertion onto device-side secure storage such that correct recovery can only be undertaken on the particular mobile device on which computations were previously undertaken.