***D. Password-change phase***

The proposed scheme allows a legitimated embedded device to change the password periodically, thereby ensuring security. To change the password, the smart meter () first perform authentication and authorization and prove their genuineness (See Fig. 1). The details of the password change are as follows:

***Step 1.*** : The authorized legitimated embedded device selects a new password and then recomputes the hashed identity and public key (=. Subsequently, it sends the updated <to SP through a trusted public channel by using the session key .

***Step 2***. : Furthermore, SP receive updated parameters < and then SP selects a random numberand then recomputes all parameters ( =h(R||||s )s, ,,, *T=h*(*||||s* )*A=*  which are mentioned in registration Subsection III*.B*. Subsequently, *TS* stores the parameters <> in the server database and sends the updated to the server *TS* through an open trusted channel by using the session key .

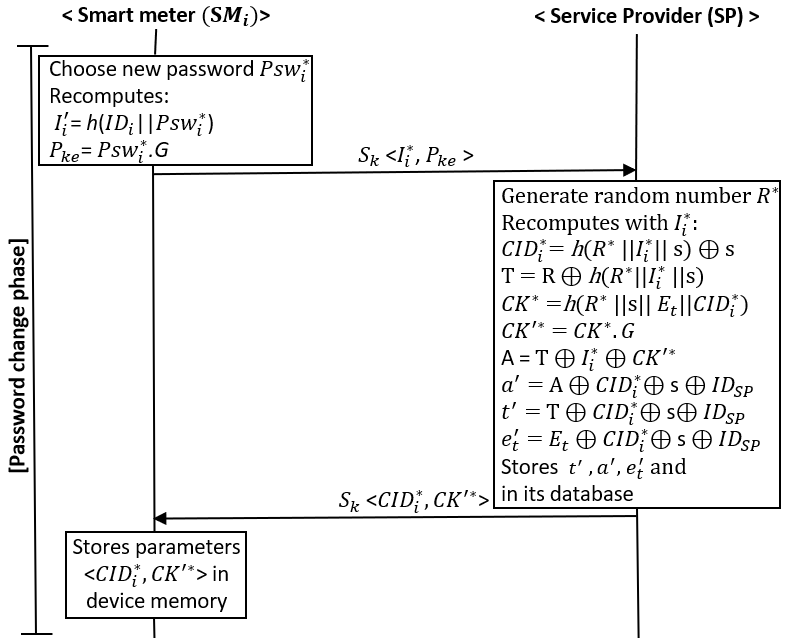


Fig.1. Password-change phase