D. *Password-change phase*

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

Step 1. $\boldsymbol{SM_i} \rightarrow$ **SP** : $< I_i^*, P_{ke}^* >$. The authorized legitimated embedded device (SM_i) selects a new password Psw_i^* and then recomputes the hashed identity ($I_i^* = H(ID_i \,||Psw_i^*\,)$) and public key ($P_{ke}^*$= $Psw_i^*.G$). Subsequently, it sends the updated <I_i^*, P_{ke}^* >to SP through a trusted public channel by using the session key S_K.

Step 2. **SP** → $\boldsymbol{SM_i}$: $< CID_i^*, CK'^* >$. Furthermore, SP receive updated parameters <I_i^*, P_{ke}^* > and then SP selects a random number $R^*$and then recomputes all parameters ($CID_i{}^*$ =h(R|| I_i^* ||s) ⊕ s, $CID_i{}'^* = CID_i{}^*.\mathrm{G}$, $CK^* = h(R^*||s||E_t||CID_i{}^*)$, $CK^{*'} = CK^*.\mathrm{G}$, T= $R^* \oplus h(R^* \,||\, I_i^* \,||s\,)$, A= $T \oplus I_i^* \oplus CK^{*'}$, $t' = T \oplus CID_i{}^* \oplus$ s $\oplus ID_{TS}$, $a' = A \oplus CID_i{}^* \oplus$ s ⊕ ID_{TS}, and $e_t' = E_t \oplus CID_i{}^* \oplus$ s $\oplus ID_{TS}$) which are mentioned in registration Subsection III.*B*. Subsequently, *TS* stores the parameters <t', a', e_t'> in the server database and sends the updated $< CID_i{}^*$, $CK^{*'} >$ to the server *TS* through an open trusted channel by using the session key (S_K).

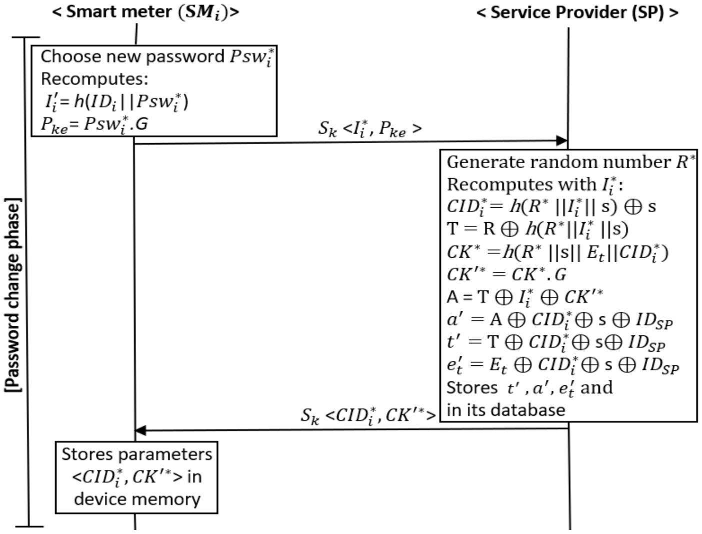
< Smart meter (SM_i)>
< Service Provider (SP) >
[Password change phase]
Choose new password Psw_i^*
Recomputes:
$I_i' = h(ID_i\,|\,|Psw_i^*)$
$P_{ke} = Psw_i^*.G$
S_k <I_i^*, P_{ke} >
Generate random number R^*
Recomputes with I_i^*:
$CID_i^* = h(R^*\,||I_i^*||\,\mathrm{s}) \oplus \mathrm{s}$
$\mathrm{T} = \mathrm{R} \oplus h(R^*||I_i^*\,||\mathrm{s})$
$CK^* = h(R^*\,||\mathrm{s}||\,E_t||CID_i^*)$
$CK'^* = CK^*.G$
A = T $\oplus I_i^* \oplus CK'^*$
$a' = \mathrm{A} \oplus CID_i^* \oplus \mathrm{s} \oplus ID_{SP}$
$t' = \mathrm{T} \oplus CID_i^* \oplus \mathrm{s} \oplus ID_{SP}$
$e_t' = E_t \oplus CID_i^* \oplus \mathrm{s} \oplus ID_{SP}$
Stores t', a', e_t' and
in its database
S_k <CID_i^*, CK'^*>
Stores parameters
<CID_i^*, CK'^*> in
device memory

Fig.1. Password-change phase