Unmanned Device Service Verifier $IDdev_k$ challenge index n $n, IDdev_k$ nonce bb $C_i' \leftarrow n \oplus b$ $C_i \leftarrow n \oplus b$ $R_i' \leftarrow PUF(C')$ $R_i \leftarrow CRP(C_i, R_i)$ from database $DB_{crp}(IDdev_k)$ $(K_i', hl_i') \leftarrow FEgen(R_i')$ $Auth'_i \leftarrow Senc((R'_i, ||hl'_i||K'_i), C'_i)$ $Auth'_i, hl'_i$ $K_i \leftarrow FE_{rep}(R_i, hl_i')$ $Auth_i \leftarrow Denc((R_i'||hl_i'||K_i), C_i)$ $HD(R_i', R_i) < \alpha$ $Auth_{i+1} \leftarrow h(Auth_i||C_i||R_i||K_i)$ $Key \leftarrow TRNG()$ $Keygen \leftarrow (Key, C_i)$ $Auth_{i+1}, KeyEx$ $Auth'_{i+1} \leftarrow h(Auth'_i||C'_i||R'_i||K'_i)$ $Auth_{i+1} == ?Auth'_{i+1}$ $Key' \leftarrow Denc(Keygen, C_i')$ $Auth'_{i+2} \leftarrow h(Keygen, h(Auth'_{i+1} \oplus Key'))$ $Auth'_{i+2}$ $Auth_{i+2} \leftarrow h(Keygen, h(Auth_{i+1} \oplus Key))$ $Auth_{i+2} == ?Auth'_{i+2}$

Figure 1: Authentication process