$PMSI, P_{new}, \kappa, \mathcal{K}, SQN$

$\mathrm{S} = \{s = \langle i, \mathcal{K}, SQN, \kappa, p, p', p'', f_{p'} \rangle | \forall i \in I\}$

SIM

SN

HN

identity request

~~update $PMSI \leftarrow P_{new}$~~
update $q \leftarrow P_{new}$
it is allowed to update $q \leftarrow PMSI$

identity response (q)

q

$i, \mathcal{K}, SQN, \kappa, p, p', p'', f_{p'} \leftarrow s \in S$ where $s_p = q \vee s_{p'} = q \vee s_{p''} = q$

~~if $s_{p'} = PMSI$ then~~
~~update $s_p \leftarrow s_{p'}$~~
~~update $s_{p'} \leftarrow \{0,1\}^{34} \notin \{ s_p, s_{p'} | \forall s \in S\}$~~
$p\_in\_RAND = g(q, s_i, s_p, s_{p'}, s_{p''}, f_p)$
$RAND \leftarrow E_\kappa (u = (p\_in\_RAND, SQN))$

BOX A

authentication request $(RAND, AUTN)$

$RAND, AUTN, XRES, CK, IK$

BOX B

$u \leftarrow E_\kappa^{-1}(RAND)$
verify $XSQN = u_{SQN}$

~~update $P_{new} \leftarrow u_{p'}$~~
if $u_{p\_in\_RAND} \notin \{i, PMSI, P_new\}$
update $PMSI \leftarrow P_{new}$
update $P_{new} \leftarrow u_{p\_in\_RAND}$

authentication response ($SRES$)

verify $SRES = XRES$

encrypted with CK

authenticity protected with IK

location update (q)

$i, \mathcal{K}, SQN, \kappa, p, p', p'', f_{p'} \leftarrow s \in S$ where $s_p = q \vee s_{p'} = q \vee s_{p''} = q$
$forget\_p, flag\_toggle = h(q, s_i, s_p, s_{p'}, s_{p''}, f_{p'})$
if $forget\_p = true$ then
update $s_p \leftarrow s_{p'}$
update $s_{p'} \leftarrow s_{p''}$
update $s_{p''} \leftarrow null$
if $flag\_toggle = true$ then
toggle $f_{p'}$