Mobile user
(U_{ID}, T_{ID}, key)

LEO
(LEO_{ID})

NCC
(x, V, T_{ID})

Input U_{ID}
$sk = h(key, T_{ID})$
$mac_U = MAC_{key}(U_{ID}, sk)$

T_{ID}, mac_U

T_{ID}, mac_U, LEO_{ID}

Verify LEO_{ID}
Find $\{V, T_{ID}\}$
$U'_{ID} = V \oplus h(T_{ID}, x)$
$key' = h(U'_{ID}, x)$
$sk' = h(key', T_{ID})$
$mac'_U = MAC_{key'}(U'_{ID}, sk')$
Verify $mac'_U \stackrel{?}{=} mac_U$
Generate T_{IDnew}
$c = h(sk') \oplus T_{IDnew}$
$mac_{NCC} = MAC_{sk'}(T_{IDnew})$
Replace T_{ID} with T_{IDnew}

c, mac_{NCC}

c, mac_{NCC}, LEO_{ID}

$T'_{IDnew} = c \oplus h(sk)$
$mac'_{NCC} = MAC_{sk}(T'_{IDnew})$
Verify $mac'_{NCC} = mac_{NCC}$
Replace T_{ID} with T'_{IDnew}

Common session key $sk = h(key, T_{ID})$