Mobile user

NCC
(x)

Select U_{ID}

U_{ID}

Generate T_{ID}
$key = h(U_{ID}, x)$
Store $\{T_{ID}, key\}$ onto U's smart card
$V = U_{ID} \oplus h(T_{ID}, x)$
Store $\{V, T_{ID}\}$ in the verification table

Smart card (T_{ID}, key)

[Secure Channel]