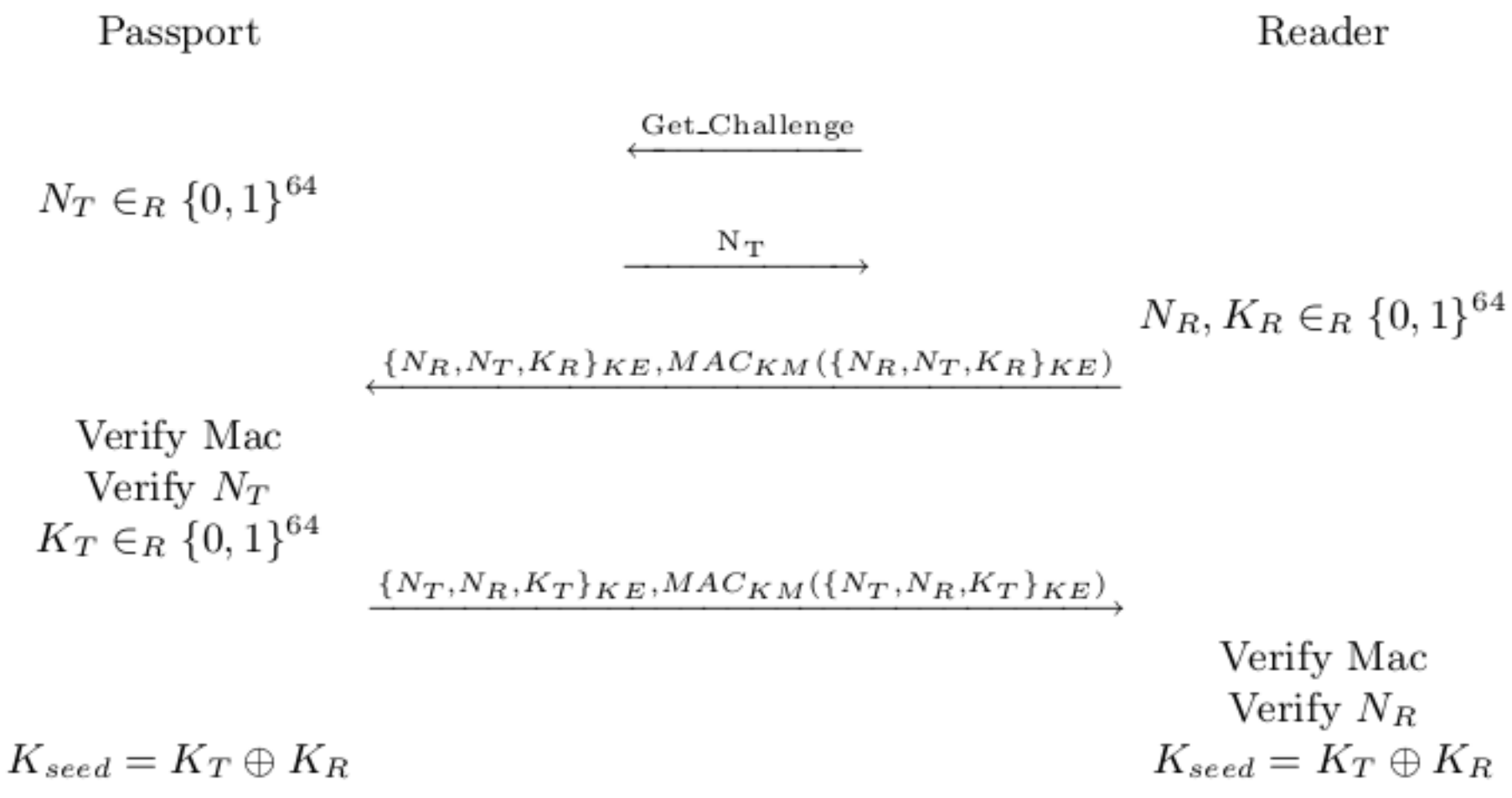
Passport
Reader
Get_Challenge
$N_T \in_R \{0,1\}^{64}$
N_T
$N_R, K_R \in_R \{0,1\}^{64}$
$\{N_R, N_T, K_R\}_{KE}, MAC_{KM}(\{N_R, N_T, K_R\}_{KE})$
Verify Mac
Verify N_T
$K_T \in_R \{0,1\}^{64}$
$\{N_T, N_R, K_T\}_{KE}, MAC_{KM}(\{N_T, N_R, K_T\}_{KE})$
Verify Mac
Verify N_R
$K_{seed} = K_T \oplus K_R$
$K_{seed} = K_T \oplus K_R$