Reader	**Tag**
ID_R, k_R^t, k_R^{t+1}	ID_R, k_{tag}

Fetch TS, $Data$ from server
Generate n_R
$D \leftarrow Data \oplus n_R$
$I \leftarrow ID_R \oplus h(TS \oplus n_R)$
$\delta_1 \leftarrow h(ID_R \oplus k_R^t) \oplus n_R$
$\delta_2 \leftarrow h(ID_R \oplus k_R^{t+1}) \oplus n_R$

$\xrightarrow{TS, D, I, \delta_1, \delta_2}$

$n' \leftarrow \delta_1 \oplus h(ID_R \oplus k_{tag})$

if $ID_R = I \oplus h(TS \oplus n')$:
  if $n' = (n')^{t-1}$: **abort**
  else: $k_{tag} \leftarrow h(k_{tag})$
else:
  $n' \leftarrow \delta_2 \oplus h(ID_R \oplus k_{tag})$
  if $ID_R \neq I \oplus h(TS \oplus n')$ **or**
    $n' = (n')^{t-1}$: **abort**
$D \leftarrow f(D \oplus n')$

$\xleftarrow{D \oplus n'}$