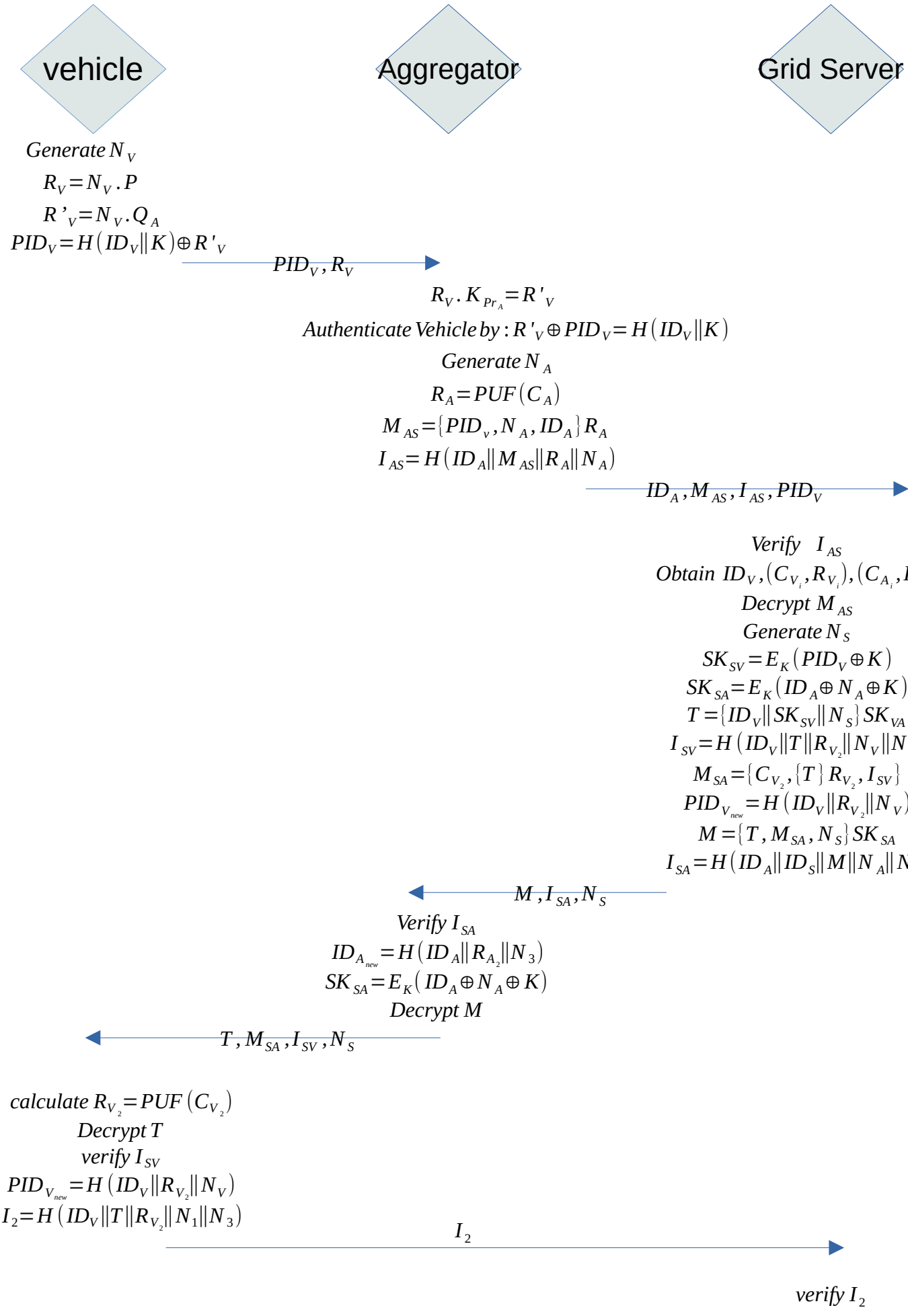
vehicle
Aggregator
Grid Server
Generate N_V
$R_V = N_V . P$
$R'_V = N_V . Q_A$
$PID_V = H(ID_V || K) \oplus R'_V$
PID_V, R_V
$R_V . K_{Pr_A} = R'_V$
Authenticate Vehicle by : $R'_V \oplus PID_V = H(ID_V || K)$
Generate N_A
$R_A = PUF(C_A)$
$M_{AS} = \{PID_v, N_A, ID_A\} R_A$
$I_{AS} = H(ID_A || M_{AS} || R_A || N_A)$
$ID_A, M_{AS}, I_{AS}, PID_V$
Verify I_{AS}
Obtain $ID_V, (C_{V_i}, R_{V_i}), (C_{A_i}, R_{A_i})$
Decrypt M_{AS}
Generate N_S
$SK_{SV} = E_K(PID_V \oplus K)$
$SK_{SA} = E_K(ID_A \oplus N_A \oplus K)$
$T = \{ID_V || SK_{SV} || N_S\} SK_{VA}$
$I_{SV} = H(ID_V || T || R_{V_2} || N_V || N_S)$
$M_{SA} = \{C_{V_2}, \{T\} R_{V_2}, I_{SV}\}$
$PID_{V_{new}} = H(ID_V || R_{V_2} || N_V)$
$M = \{T, M_{SA}, N_S\} SK_{SA}$
$I_{SA} = H(ID_A || ID_S || M || N_A || N_S)$
M, I_{SA}, N_S
Verify I_{SA}
$ID_{A_{new}} = H(ID_A || R_{A_2} || N_3)$
$SK_{SA} = E_K(ID_A \oplus N_A \oplus K)$
Decrypt M
T, M_{SA}, I_{SV}, N_S
calculate $R_{V_2} = PUF(C_{V_2})$
Decrypt T
verify I_{SV}
$PID_{V_{new}} = H(ID_V || R_{V_2} || N_V)$
$I_2 = H(ID_V || T || R_{V_2} || N_1 || N_3)$
I_2
verify I_2