

(1) $PU_a \parallel ID_A$



A



B

(2) $E(PU_a, K_s)$