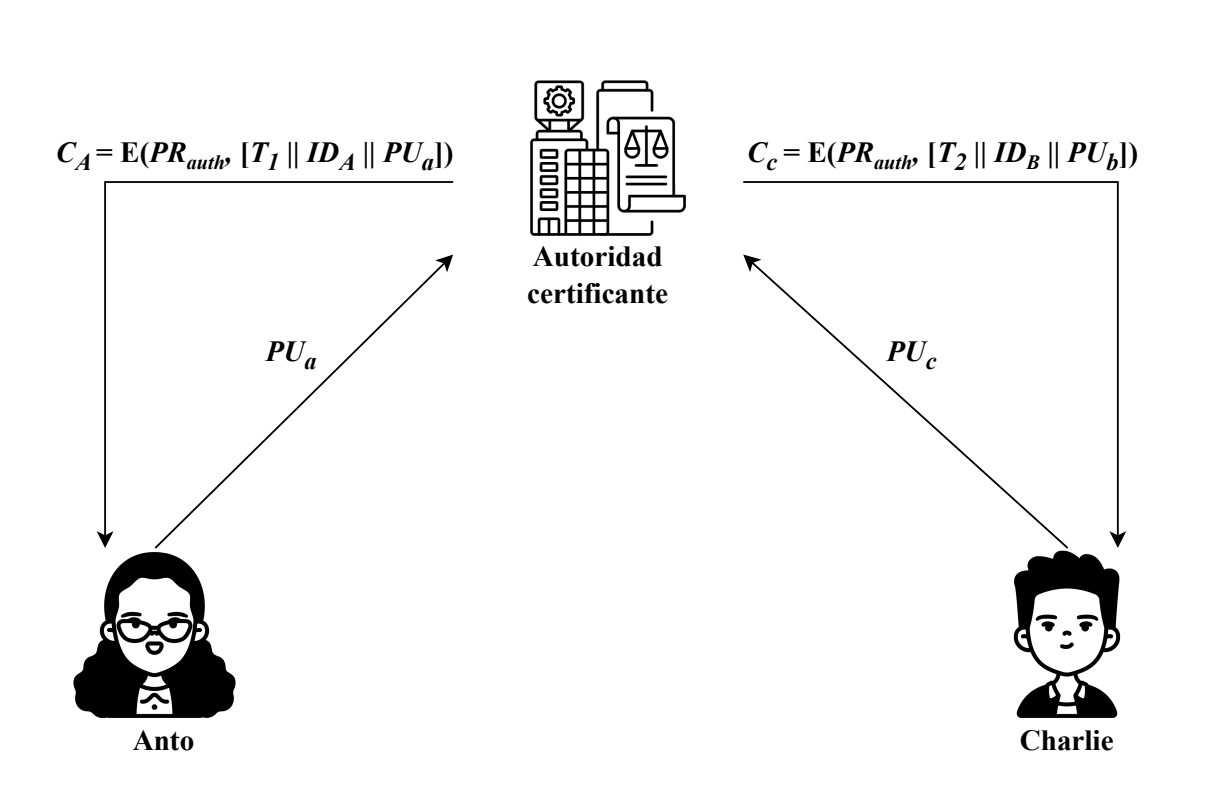
$C_A = \mathrm{E}(PR_{auth}, [T_1 \| ID_A \| PU_a])$
$C_c = \mathrm{E}(PR_{auth}, [T_2 \| ID_B \| PU_b])$
Autoridad certificante
PU_a
PU_c
Anto
Charlie