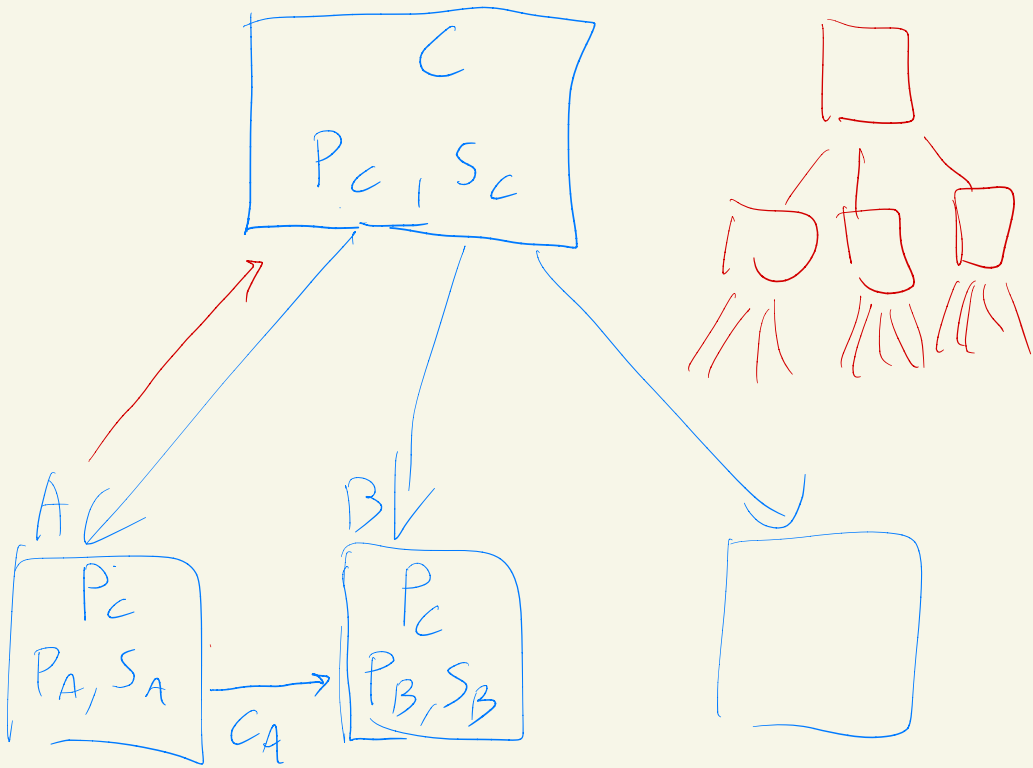


# PKI (Versign)



Certificados para A

$$\text{DEC}(S_c, \text{Enc}(P_c, m)) = m$$

$$\text{Enc}(P_c, \text{DEC}(S_c, m)) = m$$

$$C_A = \text{DEC}(S_c, \text{"la clave pública de A es } P_A\text{"})$$