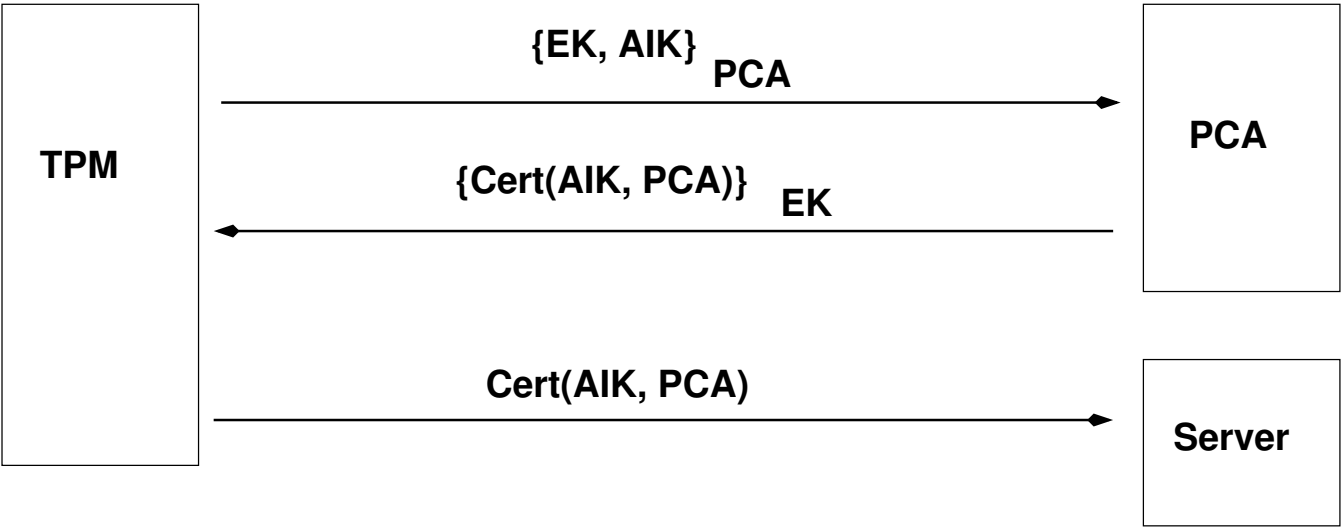
TPM
{EK, AIK}
PCA
PCA
{Cert(AIK, PCA)}
EK
Cert(AIK, PCA)
Server