

Why not?



K_{SB}, K_{pB}

$\text{Sign}_{skB}(\text{"I'm Bob"}, K_{pB})$



K_{SM}, K_{pM}

$\text{Sign}_{skM}(\text{"I'm Bob"}, K_{pM})$

Trust Models