Potential shared secret sharing

1. A generates random K
2. A $\xrightarrow{E(P_B, K)}$ B

Achieves
- A + B share a secret
- Nobody else has it

But: A got to choose the secret
Protocol 1: Just DH

\[ a \overset{A}{\rightarrow} g^a \mod p \overset{B}{\leftarrow} g^b \mod p \]

Bad: A1TM
Protocol 2:

\[ K \xrightarrow{E_{PB,K}} A \xrightarrow{} B \]

Bad: only A determines the key
Protocol 3:

1. DH

2. Challenge + response w/ certificate
cert

\[
E(S_{\text{CA}}, H(\text{TBS}))
\]

Subject: bob.com
Public key: PB

TBS "to be signed"

(If this is legit, this is what it looks like)

[Scan only CA has it]
A "validates" this cert. If yes, somebody with $S_{CA}$ created the signature.

1. $h = H(TBS)$
2. $x = E(P_{CA}, \text{sig})$
3. $x == h$ ?