Public-key Infrastructure (PKI).

- How to distribute public keys.

$(pk, sk) \leftarrow KGen(1^n)$, $\rightarrow$ PKE, $\rightleftarrows$ DS } Revolution of PKC.

Public key cryptography is used to securely distribute public keys.

We have to invest (one-time) for generating $\langle pk, sk \rangle$ pair which is used to bootstrap the generation of a number of $\langle pk, sk \rangle$ pair.

Charlie $\rightarrow \langle pk_C, sk_C \rangle$. Bob has generated a public key pk_B, and a secret key sk_B.

Charlie knows the public key pk_B of Bob.

$$Cert_{C \rightarrow B} = Sign_{sk_C}(\text{'Bob's public key is } pk_B).$$

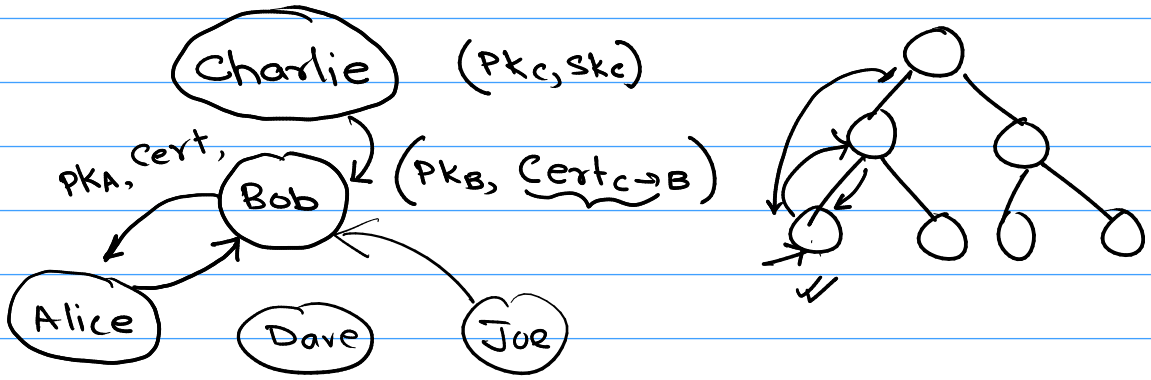
Alice knows the public key of charlie, but does not know the public key of Bob.
Alice trusts charlie.

Bob is trying to communicate with Alice.

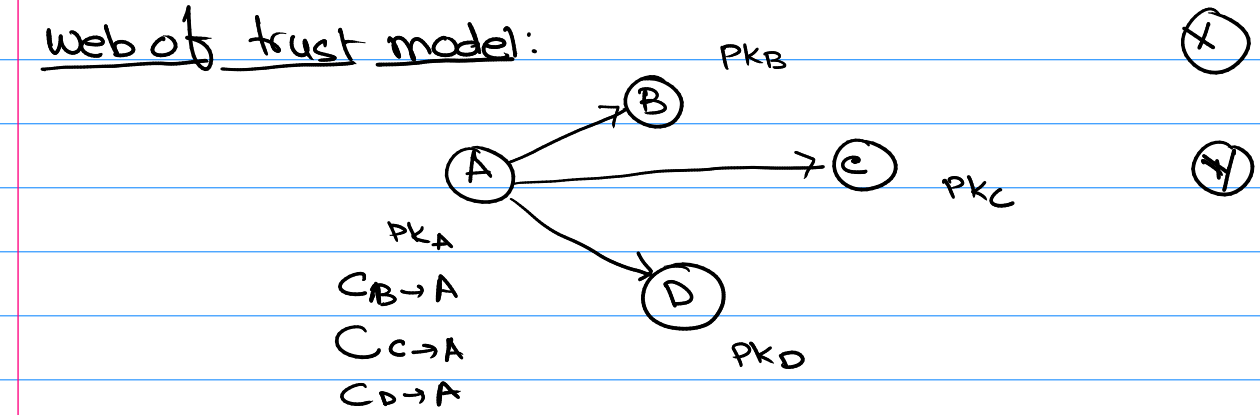
(i) Single CA model - Certifying Authority.
(ii) Multiple CA. $\rightarrow X$, $\rightarrow Y$, $\rightarrow Z$ $\leftarrow$ Bob $\{pk_X, C_{X \rightarrow B}\}$, $\{pk_Y, C_{Y \rightarrow B}\}$, $\{pk_Z, C_{Z \rightarrow B}\}$.

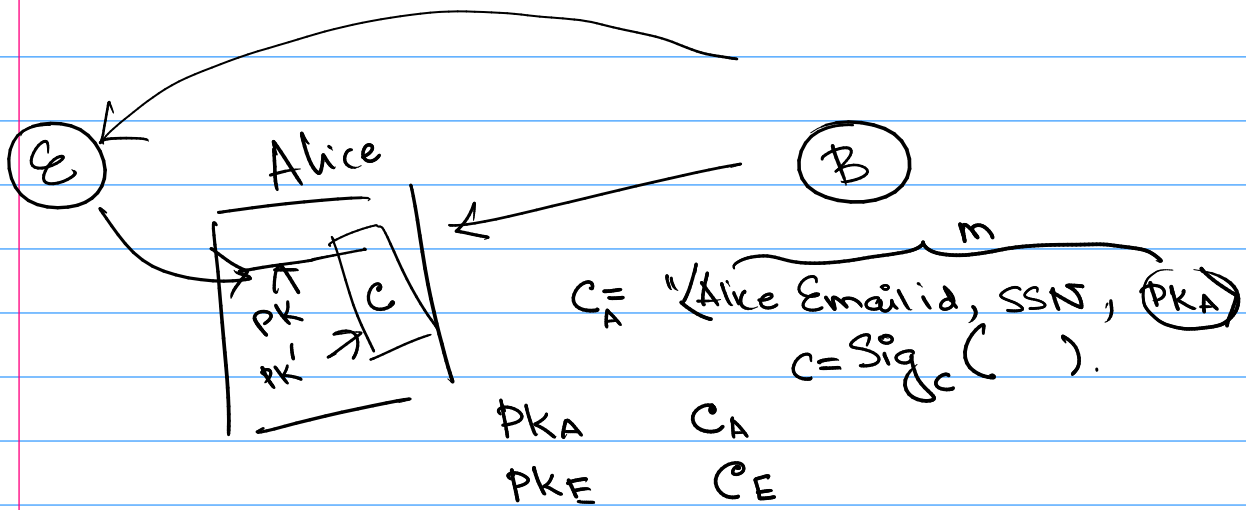
Alice Dave

Delegation and Certificate chains:



Web of trust model:





Invalidating Certificate.

$Cert_{C \to B} = Sign_{SK_C}$ (Bob's public key is PK_B, date).

$Cert_{C \to B} = Sign_{SK_C}$ (" , ####)