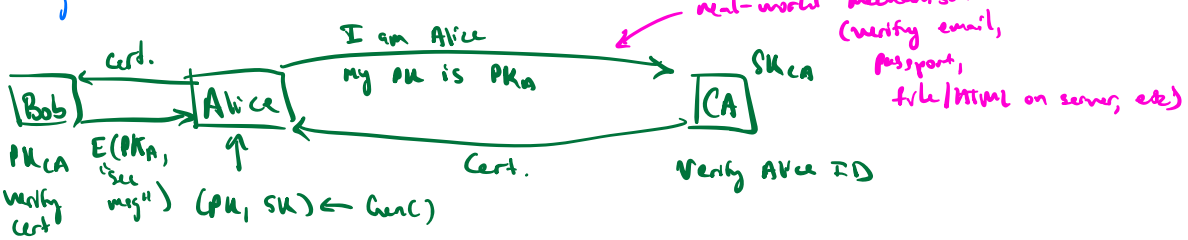
Public Key Mgmt: Certificates

How does Bob obtain Alice's PK_A?

Single domain cert. auth. (CA)



Cert: Binds PK_A to physical identity of Alice

$$\text{Cert} = \left[\text{issuer name} \mid \text{subject name} \mid PK_A \mid \text{validity period} \mid \ldots \right] + \left[\text{CA's sig on pre-cert} \right]$$

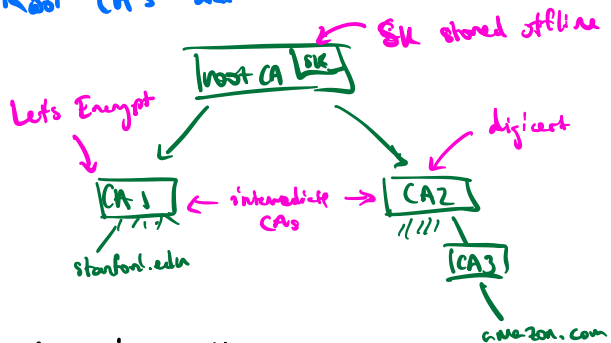
issuer name → CA; subject name → Alice; validity period → Exp. date

pre-cert

Notes.

1. Alice talks to CA during keygen
2. CA does not have Alice's SK!
3. Everyone needs PK_{CA} to verify certs.

Root CA's and intermediate CA's



Total of 60 root CAs, 1200 root CAs worldwide

Amazon's Cert:

$$\left[(\text{amazon.com} \mid PK_A \mid CA_3)_{\text{sig}},\ (CA_3 \mid PK_3 \mid CA_2)_{\text{sig}},\ (CA_2 \mid PK_2)_{\text{root sig}} \right]$$

Cert. chain of depth 3